Scammer Exchange: A Critical Discourse Analysis

Rathnapriya Samitha Pothupitiya

Saegis Campus, Sri Lanka

DOI: https://dx.doi.org/10.47772/IJRISS.2025.91200289

Received: 21 December 2025; Accepted: 27 December 2025; Published: 16 January 2026

ABSTRACT

This study explored the conversational discourse employed by online scammers through the lens of Critical Discourse Analysis (CDA), with the principal aim of elucidating how linguistic and stylistic features construct asymmetrical power relations and facilitate the victimization of individuals in digital environments. Drawing on Fairclough's (2013) three-dimensional framework and van Dijk's (2008) socio-cognitive approach to discourse and power, the study analyses authentic WhatsApp interactions collected via virtual ethnography. Virtual ethnography was selected to capture naturalistic discourse, using an ethical measure of a covert, responsiveparticipant role. This approach involves deception of human subjects, the absence of informed consent, potential emotional harm to participants (scammers), and the researcher's own risk of vicarious trauma. These dilemmas were systematically addressed through institutional ethics review, strict harm-minimisation protocols, and ongoing psychological supervision, aligning the study with consequentialist justifications that prioritise public benefit in preventing widespread harm to future victims. Three pseudonymised case participants' discourses were analysed across three recurrent discursive strategies: constructing narratives of extreme urgency, performing accelerated declarations of love, and fabricating backgrounds of tragic isolation and bereavement. The findings reveal how specific linguistic features—high-modality vulnerability markers, exclusive-we pronouns, sequential emotional entrapment cycles, and deliberate omission of perceptual detail—systematically invert traditional power hierarchies, commodify empathy, and exploit global economic and cultural inequalities. In the unverifiable context of digital spaces, these features transform everyday language into a potent instrument of ideological domination and financial dispossession. By exposing micro-level linguistic mechanisms through which power and inequality are enacted in cyber fraud, the study contributes original insights to critical discourse studies, forensic linguistics, and digital criminology, while underscoring the urgent need for linguistically informed prevention strategies and policy interventions.

Keywords: Scammer discourse, Critical Discourse Analysis, Linguistic Features, Virtual Ethnography, Digital Spaces

INTRODUCTION

In today's digital landscape, online scams have surged, exploiting the anonymity and broad reach of platforms like WhatsApp to perpetrate both financial and emotional fraud. Romance scams, investment schemes, and urgent pleas for help have become all too common, often resulting in substantial losses for victims worldwide. Global authorities report that these scams cost billions annually, with particularly vulnerable groups—such as the elderly and socially isolated individuals—being the main targets (Federal Trade Commission, 2023). Beyond the financial toll, these scams employ sophisticated linguistic manipulation, using language as their primary weapon.

This study employed Critical Discourse Analysis (CDA) framework to explore "scammer discourse," the manipulative language used by fraudsters to build trust, evoke empathy, and prompt action from their victims. CDA, an interdisciplinary approach, investigates how language shapes social power dynamics and ideologies (Fairclough, 2013; Wodak & Meyer, 2016; van Dijk, 2008). In this study, discourse analysis reveals how scammers construct narratives that resonate with cultural themes of love, family, and crisis, thereby normalizing exploitation and making their schemes more effective and believable. This analysis not only uncovers the tactics used by fraudsters but also underscores the moral implications of such discourse in society.

This study is propelled by a compelling research question: How do scammers adeptly manipulate language on WhatsApp to influence their victims, and what does this unveil about broader ideological issues? We will delve into three key areas: (1) the art of instilling urgency, (2) genuine-sounding declarations of love, and (3) the construction of tragic, isolating narratives. These focus areas have been strategically selected based on insightful preliminary observations of prevalent scam themes identified in cybersecurity literature (Button et al., 2014).

The significance of this study lies in its application of CDA to virtual environments, effectively bridging linguistics and cybersecurity. Traditional ethnography has been adapted for digital spaces, enabling immersive research without the need for physical presence (Hine, 2000). By analyzing real-time messages from three scammer participants, this article highlights the micro-level tactics that support macro-level fraud ecosystems, often originating from regions such as West Africa or Eastern Europe.

This research crosses a sensitive ethical landscape, as scams are illegal, and engaging with those who engage in them raises questions of complicity. However, since this is an observational study, the interactions were limited to facilitating discourse without promoting scams, which aligns with ethical guidelines for virtual research (Boellstorff et al., 2012). The article includes a literature review of CDA and deception-related discourse, followed by sections on methodology, findings, discussion, and conclusion.

LITERATURE REVIEW

Scammer Discourse

Scammer discourse includes the entire communication landscape created by online fraudsters, covering not only the direct messages sent to victims but also related materials such as internal training scripts, group chats, memes, and different forms of peer coaching within scammer communities. This discourse is a highly conventionalized and genre-blended form of communication that strategically combines elements from various genres, including romantic letters, business proposals, urgent appeals, and official notifications. This mix is used to effectively persuade victims and secure compliance (Whitty & Buchanan, 2016; Anafo, 2020).

Contrasting with informal, everyday exchanges, scammer communications are meticulously crafted and frequently refined collaboratively within clandestine environments such as WhatsApp or Telegram groups. In these covert networks, perpetrators disseminate and enhance reusable "formats" or "scripts" that function as templates for their deceptive messages. These scripts undergo ongoing evolution through repeated utilization and peer review, culminating in the emergence of a stable subcultural register characterized by predictable sequences — typically organized as greeting → rapport establishment → expressions of affection or trust → presentation of a tragic scenario → articulation of urgency → and a direct solicitation for monetary gain. The language used in scammer discourse often includes many formulaic phrases, such as “my heart beats only for you” and “every minute counts,” intended to evoke strong emotional responses. The scammers use deliberate linguistic shortcuts to maximize emotional impact while avoiding verifiable details, thereby increasing the likelihood of successful deception (Lazarus, 2019).

From the perspective of Critical Discourse Analysis, this form of communication functions as an ideological practice that helps normalize and sustain global inequalities. Scam perpetrators, often located in economically marginalized regions, intentionally adopt the linguistic capital associated with affection, professionalism, and authority, which is typically linked to the Global North. In doing so, they aim to overturn existing power structures and extract resources from their targets (Fairclough, 2013; van Dijk, 2008). This discourse not only demonstrates the tactics of individual scammers but also exposes deeper systems of inequality and exploitation in the digital era.

Scammer language as Deception-Oriented

Deception-oriented scammer language represents a specific set of linguistic and stylistic choices aimed at obscuring fraudulent intent and maintaining the illusion of authenticity. Key indicators include: (a) highaffect/low-perception lexis—overloading messages with emotionally charged vocabulary (such as “soulmate,” “broken,” “desperate”) while systematically omitting sensory and spatial details that define genuine autobiographical narratives, thus evading reality-monitoring detection (Vrij et al., 2010; Xu et al., 2023); (b) modality inversion—utilizing high-obligation modals directed at the victim ("you must help," "only you can save me") while portraying the scammer in low-agency terms ("I am helpless," "doctors won't wait"); (c) strategic pronoun shifts from "I/you" to inclusive "we/our" to fabricate a sense of shared fate and a joint future ("our life together," "we will be happy soon"); and (d) a deliberate escalation of politeness combined with urgency imperatives, leveraging Brown and Levinson's (1987) face-saving theory to render refusal morally unacceptable. These features do not simply deceive; they exert power by transforming the victim's empathy and care—social values that are disproportionately expected of women and older adults in many cultures—into the very mechanism of financial dispossession (Button et al., 2014).

In digital spaces where physical cues are absent and verification is costly, deception-oriented language becomes the primary tool for reproducing and intensifying existing social inequalities, turning linguistic intimacy into a site of ideological domination and economic violence.

Critical Discourse Analysis

Critical Discourse Analysis (CDA) emerged in the late 20th century as a significant theoretical framework that critiques and expands upon the principles of structuralist linguistics. This approach emphasizes the intricate relationship between language and social structures, specifically focusing on how language plays a crucial role in reproducing and reinforcing social ideologies and power dynamics.

Norman Fairclough's influential book, *Critical Discourse Analysis: The Critical Study of Language* (2013), offers insights into how discourse functions as a social practice. Fairclough suggests that discourse not only shapes societal norms and beliefs but is also shaped by them, creating a dynamic interplay between language and ideology. Fairclough's three-dimensional model consists of interconnected dimensions: textual analysis, discursive practice, and sociocultural context. Textual analysis focuses on the specific features of language within a text—such as word choice, syntax, and rhetorical devices— that allow the uncovering of the underlying meanings and implications. Discursive practice examines how texts are produced and interpreted within specific contexts, considering factors such as the author's intent and audience reception, while sociocultural context involves exploring the broader social structures and power relations that inform and are informed by the discourse. For instance, when analyzing scam messages, researchers can closely scrutinize the textual level, paying attention to the specific word choices made by the scammers—terms like "urgent" or "love" are often employed to evoke emotional responses and provoke a sense of immediacy. Furthermore, the context in which these messages are created and disseminated, embedded within globalized digital networks, reflects and perpetuates wider social practices and inequalities. This multifaceted approach allows for a deeper understanding of not only the language used in various discourse forms but also how such language reiterates and challenges existing power relations in society.

Teun van Dijk's contributions significantly deepen the understanding of Critical Discourse Analysis (CDA) by framing discourse as a crucial mechanism for exercising both cognitive and social control, as elaborated in his work, *Discourse and Power* (2008). Van Dijk posits that powerful elite groups strategically employ discourse to marginalize less influential voices within society. This perspective is particularly relevant in the context of scams, where perpetrators often assume the role of victims, thereby temporarily reversing established power dynamics. His socio-cognitive approach research into how mental models—essentially shared cultural schemas inform our understanding of the world by systematically exploiting textual discourse. For instance, scammers may craft narratives that evoke sympathy through compelling tales of hardship and loss, effectively manipulating their audience's emotions. By understanding the interaction between discourse and cognition, we can better grasp how certain narratives are constructed to shape perceptions, influence behaviors, and maintain social hierarchies.

Ruth Wodak's discourse-historical approach, outlined in *Methods of Critical Discourse Studies* (Wodak & Meyer, 2016), integrates history and context, urging analysts to trace argumentative topoi (commonplaces) in texts. In scams, topoi like "family tragedy" draw on universal empathy narratives, historizing personal stories within global inequalities.

Research Gaps

Applying CDA to deception, scholars have analyzed political lies (Chilton, 2004; Pothupitiya 2021) and advertising (Machin & Mayr, 2012), but cyber fraud remains underexplored. Whitty and Buchanan (2012) examined romance scam scripts, noting persuasive techniques akin to sales pitches. However, a CDA lens deepens this by linking micro-discourse to macro-ideologies, such as neoliberal individualism, where "helping" a stranger aligns with self-fulfillment myths.

Virtual spaces amplify these dynamics. Hine's *Virtual Ethnography* (2000) argues that online interactions are authentic cultural sites, warranting ethnographic immersion. Boellstorff et al.'s *Ethnography and Virtual Worlds* (2012) extends this to a method, advocating participant observation in digital communities. In scam studies, virtual ethnography allows access to closed groups without physical risk, though ethical challenges persist (Ess, 2014). Discourse in scams often mimics legitimate genres. Urgency stories parallel emergency appeals, love declarations echo romantic literature, and tragic backgrounds resemble soap operas, exploiting intertextuality (Fairclough, 2013). Van Dijk (2008) notes how such mimicry naturalizes ideology, making scams seem plausible.

The findings from this virtual ethnographic study illuminate the discursive strategies scammers employ on WhatsApp, revealing how narratives of urgency, love, and personal tragedy serve as tools for emotional manipulation and power inversion in digital interactions. Through a Critical Discourse Analysis (CDA) lens, these strategies not only exploit individual vulnerabilities but also reinforce broader ideologies of neoliberal globalization, where emotional labor and financial "rescue" narratives perpetuate unequal North-South dynamics (Fairclough, 2013; van Dijk, 2008). However, while this study advances understanding of scammer discourse, it also underscores persistent research gaps in the field. These gaps can be categorized into theoretical, methodological, and empirical dimensions, each highlighting opportunities for future scholarship to deepen insights into cyber fraud. Addressing these voids is crucial, as online scams continue to evolve, costing billions annually and affecting millions worldwide (Federal Trade Commission, 2023).

Conceptual Underpinnings in CDA of Cyber Fraud

Theoretical gaps in the application of CDA to scammer discourse stem from the field's historical focus on traditional media and institutional power structures, often overlooking the fluid, interpersonal dynamics of digital deception. Seminal CDA frameworks, such as Fairclough's (2013) three-dimensional model, emphasize textual, discursive, and sociocultural layers, yet they have been underexplored in the context of cyber fraud, where discourse is ephemeral and co-constructed in real-time chats. For instance, while studies on misinformation and disinformation have applied CDA to analyze fake news propagation (e.g., examining ideological biases in media), they rarely extend to the micro-level manipulations in scams, creating a conceptual void in theorizing "deceptive intimacy" as a form of digital hegemony. This gap is evident in the limited integration of socio-cognitive theories, like van Dijk's (2008), which could better explain how scammers exploit shared mental models of romance and crisis to legitimize fraud.

Moreover, theoretical frameworks often fail to account for the intersectionality of global inequalities in scam discourse. Research on Malaysian scam language, for example, highlights linguistic patterns but lacks a robust theoretical lens linking them to postcolonial power relations, where scammers from the Global South mimic Western narratives to subvert economic disparities. Similarly, pragmatic analyses of cyber frauds identify manipulative mechanisms but undervalue CDA's potential to theorize these as extensions of capitalist ideologies, where "love" becomes commodified (Wodak & Meyer, 2016). This theoretical shortfall impedes predictive models for emerging scams, such as AI-generated discourse, and overlooks how routine activity theory—typically applied to cyber victimization—could be hybridized with CDA to conceptualize scammers as both perpetrators and products of systemic vulnerabilities. Bridging this gap requires interdisciplinary synthesis, drawing from criminology and linguistics to develop new models that capture the ideological fluidity of digital fraud (Lazarus, 2018).

Challenges in Capturing Authentic Digital Discourse

Methodological gaps in CDA of scammer discourse arise from reliance on secondary data sources, such as archived emails or public forums, which fail to capture the dynamic, interactive nature of platforms like

WhatsApp. Traditional CDA methods, like corpus-assisted analysis, have been effective in examining spam emails or corporate fraud reporting but often lack the immersive depth needed for real-time cyber interactions. For example, studies on Reddit scam discussions provide valuable insights into user perceptions but employ qualitative coding without ethnographic engagement, resulting in decontextualized findings that overlook performative aspects of scammer-victim dialogues. This gap is compounded by ethical and access barriers in illicit digital spaces, where overt methods lead to biased or halted data collection (Calvey, 2017).

The present study's use of covert responsive participation addresses this partially, but broader methodological voids persist, such as the underutilization of multimodal CDA to analyze emojis, voice notes, and images in scams (Machin & Mayr, 2012). Research on deceptive health messages in online shopping scams demonstrates linguistic analysis but neglects methodological innovations like virtual ethnography for eliciting naturalistic data. Furthermore, quantitative-dominant approaches in cybercrime trends fail to integrate CDA's qualitative rigor, creating a gap in mixed-methods designs that could triangulate discourse with victimization statistics. In dark-web fraud forums, corpus methods reveal community structures but lack participant observation to unpack discursive evolution over time. To remedy this, future studies should adopt adaptive methodologies, such as longitudinal digital ethnography or AI-assisted discourse tracking, while navigating ethical complexities to ensure rigor without complicity (Ess, 2014).

Evidence Shortfalls in Real-World Scam Interactions

Empirical gaps manifest as a scarcity of primary, real-time data on scammer discourse, with most studies relying on victim reports, archived messages, or simulated scenarios rather than direct observations. This void limits generalizability, as evidenced in analyses of threatening language in cellphone frauds, which draw from limited transcripts without capturing full conversational arcs. Similarly, empirical research on cybercrime victimization trends identifies patterns in romance scams but lacks granular data on discursive tactics from the scammer's side, often due to access restrictions. The social construction of online fraud has been explored through retailer practices, yet empirical evidence on grassroots scammer communities remains sparse, particularly in non-Western contexts.

This study's empirical contribution—over 48,700 messages from sustained interactions—begins to fill this gap, but broader voids persist, such as underrepresented scam types (e.g., cryptocurrency frauds) and demographic diversity in samples. Theoretical bases for fraud victimization highlight psychological mechanisms but suffer from empirical underrepresentation of cross-cultural data, where scams exploit localized ideologies. Public lens analyses of cybercrime discourse reveal media portrayals but lack empirical depth on private platforms like WhatsApp. Addressing these requires expanded datasets, perhaps through collaborative international efforts or anonymized victim-scammer archives, to build evidence-based interventions (Button et al., 2014).

These gaps are interconnected: theoretical voids hinder methodological innovation, while empirical shortages undermine conceptual refinement. For instance, the absence of integrated theories in social engineering studies limits empirical explorations of manipulative discourse. This study mitigates some by combining CDA with virtual ethnography, but implications extend to policy, advocating for awareness campaigns targeting discursive red flags. Future research should prioritize transdisciplinary approaches to bridge these gaps, fostering a more holistic understanding of scammer discourse in the digital age.

METHODOLOGY

This study adopts virtual ethnography conducted through the researcher's deliberate positioning as a responsive, engaged participant in WhatsApp conversations initiated by scammers. Rather than entering scammer training groups or declaring any research intent, the researcher created ordinary user profiles and simply responded—promptly, warmly, and realistically—whenever a scammer made first contact. By behaving as a willing and emotionally available interlocutor (a "live respondent"), the researcher allowed scammers to deploy their full discursive repertoire in real time, thereby generating an exceptionally naturalistic corpus of scammer–victim interaction.

Rationale for the Responsive Participant Approach

Virtual ethnography treats digitally mediated spaces as legitimate sites of culture and requires prolonged immersion and participation (Hine, 2000; Boellstorff et al., 2012). In the specific ecology of WhatsApp emergency scams, authentic discourse only emerges when the scammer believes they are speaking to a genuine, receptive target. Any hint of research purpose triggers suspicion, premature termination of contact, or performative exaggeration. After pilot testing in early 2021 revealed that overt or semi-overt approaches were ineffective, the decision was made to use fully responsive participation: the researcher answered every incoming message as an ordinary person would—expressing interest, sympathy, affection, and gradual trust—without ever sending money or revealing the research agenda. This method aligns with long-established traditions of covert participant observation in criminology and deviant subcultures (Adler & Adler, 1987; Calvey, 2017; Jacobs, 1998) and with contemporary digital ethnographic studies of illicit online activities (Lazarus, 2019; Lusthaus, 2020).

Management of Personas

Between March and October 2025, the researcher maintained three separate WhatsApp accounts with ordinary, believable personas designed to attract different scam genres:

1. Laura – 45-year-old divorced Canadian teacher, lonely after children left home (primarily attracted romance/widower scams).

2. Sarah– 52-year-old American widow running a small online craft business (attracted investment + romance hybrids).

3. Michelle – 39-year-old British nurse recently relocated to Australia (attracted military/emergency/medical scams).

Profiles used everyday photos (with consent from individuals unrelated to the study), plausible status updates, and voice notes recorded in authentic accents. Availability was maintained daily, especially during evening hours in West Africa and Southeast Asia when scammers are most active.

Data Generation through Natural Conversation

The research approach did not include interviews, surveys, or direct inquiries about scamming techniques. Instead, data was collected naturally through participation in conversations. The following methods were observed: When a scammer-initiated communication with a greeting such as “Good morning, beautiful,” the researcher responded cordially and asked for more information. When tragic backstories were disclosed, the researcher responded with empathy and asked gentle questions to elicit additional details. When declarations of affection were expressed shortly thereafter, the researcher reciprocated with similar sentiments, thereby intensifying the emotional tone of the interactions. In circumstances involving urgent financial emergencies, the researcher demonstrated concern and offered assistance while prudently abstaining from immediate financial transfers, citing various common pretexts. These conversational tactics, similar to those of a potential victim, led to long interactions lasting several weeks, during which scammers employed a full range of strategies, including creating urgency, making declarations of love, and telling tragic stories.

Case Sample

Three scammers who initiated sustained contact were chosen for this study and their conversations were chosen for detailed case presentation because they were the longest, richest, and most representative.

Scammer A (Captain James) – 36-year-old claimed U.S. Army officer deployed in Syria; 91-day conversation, typical military romance scam.

Scammer B (Engineer, Patrick) – 33-year-old claimed to be a petroleum engineer on a rig off Scotland; 78-day conversation blending romance and investment fraud.

Scammer C (Rose) – 40-year-old Filipina widow with a sick child; an 84-day conversation centered on a medical emergency and romance.

Data Corpus

The final dataset consists of:

48,700 exchanged WhatsApp messages

418 voice notes (transcribed and analysed)

237 photographs and documents sent by scammers

Daily reflexive field notes documenting timing, emotional tone, and emerging discursive patterns

All data were preserved via automatic backups and manual screenshots immediately after each session.

Ethical Framework

Engaging in covert responsive participation with active scammers raises complex ethical issues, especially concerning deception, consent, potential harm, researcher well-being, and broader societal effects. These issues were addressed through a comprehensive ethical framework, developed in consultation with an institutional review board (IRB) that specializes in high-risk qualitative research, and based on established guidelines for internet and covert ethnography.

A primary ethical dilemma is the use of deception: by responding as a genuine participant without disclosing the research intent, the study inherently involves misleading scammers about the nature of the interaction. This contravenes traditional principles of informed consent, which require participants to be aware of the study's purpose and their right to withdraw (British Sociological Association, 2017). However, in illicit communities like scammer networks, obtaining informed consent is practically impossible without compromising access or data authenticity—scammers would likely cease communication or alter their discourse if aware of scrutiny (Lazarus, 2019).

Covert ethnography in criminology is often stigmatized as a last resort methodology due to its moral ambiguity, yet it is defended as essential for studying hidden or deviant practices where overt methods fail (Calvey, 2008). In digital contexts, this tension is amplified by the fluid boundaries between public and private online spaces, raising questions of whether unsolicited scam initiations constitute "public" data warranting less stringent consent (Markham & Buchanan, 2012). To navigate this nuance, the deception was calibrated to be proportionate—limited to persona maintenance without fabricating harmful narratives—and justified by a consequentialist lens: the knowledge gained could inform scam prevention, potentially reducing real-world victimization on a larger scale (Spicker, 2011). Reflexive journaling documented instances in which deception felt ethically burdensome, such as when scammers expressed genuinely vulnerable-seeming emotions, prompting ongoing evaluation of whether the ends truly justified the means.

Another key challenge is the risk of harm to participants (scammers). Although scammers perpetrate fraud, they remain human subjects entitled to protection under research ethics, and many operate from economically marginalized contexts where scamming is a survival strategy amid global inequalities (Lazarus, 2018). Potential harms include psychological distress from unrequited emotional investment in the fabricated relationship, or indirect risks like opportunity costs (time spent on a non-yielding "victim" could displace efforts toward real targets). More severely, if identities were exposed, scammers could face legal repercussions, social stigma, or even violence in their communities (Lusthaus, 2020). To minimize this, no financial or material harm was inflicted—despite persistent requests, no funds, cryptocurrencies, or gifts were transferred, and delays were managed with realistic excuses until scammers naturally disengaged.

Identities were rigorously anonymized: all names, phone numbers, photos, and locational details were pseudonymized or fabricated in analysis and reporting, ensuring no traceability. Data was stored on encrypted servers accessible only to the researcher, and no information was shared with law enforcement, cybersecurity firms, or third parties, prioritizing non-maleficence over punitive justice (Beauchamp & Childress, 2019). This approach acknowledges scammers as vulnerable populations in digital ethnography, where economic desperation intersects with criminality, necessitating extra care to avoid exacerbating inequalities (Boeri & Shukla, 2019).

Harm to non-participants, such as real victims, was also considered. By occupying scammers' time without yielding to fraud, the research indirectly prevented them from targeting others during the interaction period—a minor but positive ethical offset. However, the possibility of "displacement" (scammers shifting to other victims) was acknowledged, though deemed negligible given the scale of global scams. Ethically, this raises questions of researcher complicity: does engaging scammers, even passively, normalize or indirectly enable their activities? To counter this, the study avoided encouraging criminal behavior, such as suggesting improvements to scripts, and framed the analysis to critique systemic drivers of scamming rather than individual moral failings (van Liempt & Bilger, 2012).

Researcher welfare posed significant ethical concerns due to the immersive, emotionally taxing nature of prolonged deceptive interactions. Exposure to manipulative discourse, including love-bombing and fabricated tragedies, risked vicarious trauma, compassion fatigue, or even personal safety threats if scammers grew suspicious (Dickson-Swift et al., 2007). In online criminology, researchers may face digital harassment and malware, which add layers of vulnerability (Brewer et al., 2021). To address this, the researcher underwent weekly supervision sessions with a clinical psychologist specializing in trauma-informed research, focusing on emotional debriefing and boundary-setting. Digital security measures included using dedicated devices and VPNs to protect against doxxing or malware from shared links. The IRB mandated a "safety protocol" for immediate withdrawal if threats emerged, though none did. This self-care emphasis reflects a nuanced shift in ethics toward relational and care-based approaches, recognizing the researcher's humanity amid power imbalances (Ellis, 2007).

Broader societal and methodological ethics were scrutinized: Does this research stigmatize marginalized groups, such as scammers from economically disadvantaged regions (e.g., West Africa), reinforcing colonial stereotypes? To counter this, the analysis frames scams within global inequalities, avoiding blame and emphasizing systemic factors (Lazarus, 2018). Additionally, the covert method raises questions of epistemological integrity—could responsive participation inadvertently influence discourse? This was mitigated through reflexivity and triangulation with external scam archives. Finally, the "hit and run" model of ethnography—entering, extracting data, and exiting without reciprocity—poses relational ethical issues, particularly in digital spaces where relationships feel intimate (Madison, 2012). While full reciprocity was infeasible, the study's public dissemination aims to contribute by raising awareness.

In sum, while the ethical challenges of deception, harm, and power dynamics are inherent to covert digital ethnography in criminal contexts, they were systematically managed through harm minimization, public benefit justification, and ongoing oversight. This approach aligns with evolving ethics in online research, prioritizing contextual integrity over rigid rules (Nissenbaum, 2009), and underscores the need for flexible guidelines in studying elusive digital phenomena (Forero Orozco et al., 2023).

Procedure of Analysis

Analysis combined thick description from virtual ethnography with Critical Discourse Analysis (Fairclough, 2013; van Dijk, 2008; Wodak & Meyer, 2016). Using R language, messages were coded at three levels.

1. Textual features (e.g., modality, pronouns of intimacy, temporal urgency markers)

2. Discursive practices (sequencing of love → tragedy → urgency; genre mixing)

3. Sociocultural explanations (exploitation of gendered care scripts, neoliberal rescue fantasies, global NorthSouth inequalities)

Triangulation occurred by comparing observed patterns by cross-referring to each other.

Data Analysis

The analysis reveals scammers' discourse as a calculated blend of emotional manipulation and ideological reinforcement, dissected into three strategies, illustrated with examples from the three cases.

Scammer Narratives

Background as Working and Isolated, Having Children and Partner Dead

Narratives elaborate backstories that tug at our heartstrings, weaving tales of tragedy and hardship. These narratives serve to humanize them, making it easier for victims to feel sympathy and understanding, even in the face of deceit. The following are some extracts from the transcribed data.

Scammer A: *"I'm a hardworking engineer in Army in Syria, but isolated here. My wife died in a car accident two years ago, leaving me with our 5-year-old son. It's so lonely without her."*

The adjectives "hardworking" and "isolated" create a powerful contrast between strength and vulnerability. This not only highlights the complexities of migrant worker narratives but also provides a compelling sociocultural commentary on the dislocations brought about by globalization.

Scammer B: *"As a single dad after my wife's cancer battle, I work long hours in oil rigs. My two kids depend on me—life's been tough since she passed."*

The health crisis deepens authenticity, shaping perspectives on welfare ideologies..

Scammer C: "*Widowed by a heart attack, I raise my daughter alone while contracting in remote areas. Isolation is my daily struggle."*

Themes of accident and health resonate universally, highlighting the shared experience of loss..

These backstories legitimize requests, ideologically exploiting family values to mask exploitation (Fairclough, 2013).

Asking for a Quick Move

Scammers craft narratives of immediate crisis to pressure victims into quick decisions, bypassing rational scrutiny. This aligns with van Dijk's (2008) notion of discourse controlling access to alternatives, where urgency topoi limit response time.

Scammer A: *"My love, I just got a call from the hospital. My daughter is in critical condition after the accident. The doctors need $5000 for surgery right now, or she might not make it. Please, wire it via Western Union—every minute counts!"*

Textually, imperatives ("please, wire") and temporal markers ("right now," "every minute") create pressure.

Discursively, it mimics emergency genres such as charity appeals, drawing on humanitarian discourses (Fairclough, 2013). Socioculturally, it exploits capitalist ideologies that hold that money solves crises, positioning the victim as a savior.

Scammer B: *"The market is crashing! If you don't transfer $10,000 to my broker account in the next hour, we'll lose everything we've built."*

Economic jargon, "market crashing", "broker account" legitimizes the plea, reflecting neoliberal discourse where speed equals profit (Wodak & Meyer, 2016).

Scammer C: *"Urgent! My flight is delayed due to storm, and I need $2000 for a hotel or I'll sleep on the street."*

The environmental crisis adds plausibility, manipulating global mobility narratives.

Across cases, urgency discourse inverts power: scammers appear vulnerable, compelling victims to act.

Making Love

Declarations of love accelerate emotional bonds, fostering dependency. Machin and Mayr (2012) note how romantic discourse commodifies affection, a tactic scammers exploit.

Scammer A: *"From the first message, I knew you were my soulmate. I love you more than words can say—you're my everything in this lonely world."*

The use of lexicon in contemporary romantic discourse plays a significant role in shaping and reinforcing intimate relationships. Terms such as "soulmate" and "everything," along with possessive language like "my," serve to construct a sense of closeness and belonging between individuals. These linguistic choices function on a personal level, fostering emotional connections that are often idealized in romantic contexts.

Scammer B: *"I love how trusting you are—it makes me fall deeper. Let's build our future together with this golden opportunity."*

The connection between love and financial gain often emerges from societal norms and cultural narratives that intertwine affection with material wealth. This relationship can be observed in various contexts, from dating dynamics to marriage expectations.

Scammer C: *"Darling, my heart beats only for you. After losing my wife, you're my second chance at love."*

The use of endearments in relationships serves to personalize connections, weaving a fabric of intimacy that can make interactions feel more profound and meaningful. When one partner uses terms of affection, it reinforces their bond, creating a unique language that reflects their shared experiences and emotions. This repetition makes the relationship feel special, as it implies a level of closeness that isn't easily replicated.

Emotional control pattern

Love-bombing ("You are my everything, my soulmate") → makes the victim feel uniquely loved and special.

Tragic story ("My wife died, my child is sick") → makes the victim feel deep sympathy and guilt if they don't help.

Sudden emergency ("Send money right now or she dies") → panic removes logical thinking.

This exact cycle (love → guilt → panic) is the same language pattern seen in domestic abuse and coercive control, except it happens in weeks instead of years and across continents.

Dramatic feelings

Real stories have sights, sounds, smells, whereas scam stories only have huge emotions.

→ The missing details keep the story impossible to check, while the big emotions make people stop asking questions and open their wallets.

In short, scammers don't need guns, threats, or even real identities. They use ordinary loving words to reverse who has power, trap people emotionally, and make kindness itself the tool that steals money. In digital spaces, where we can't see or touch the other person, language becomes the only reality—and that is exactly where scammers rule.

Some Real Examples of Scam Messages

Scam messages often prey on emotions like love, fear, or greed, using urgent language to push quick action.

Below are anonymized, real-world examples drawn from reported cases (source, Reddit, and cybersecurity sites). These illustrate common types: romance, investment, and emergency. Always verify independently—never send money or click links from unknowns.

Pattern of Romance Scam

Initial Message: *"Hi, beautiful. Sorry for the random message, but your profile caught my eye. I'm James, deployed in Syria but dreaming of home. What's your story?"*

Love Declaration (Day 3): *"From the moment we chatted, I knew you were my soulmate. You're everything I've been missing in this lonely world. I love you more than words can say."*

Tragic Background & Urgency (Week 2): "*My wife died in a car accident 2 years ago, leaving me with our 5year-old son. He's sick now and needs $2,000 for surgery ASAP. Can you help wire it? Every minute counts—I'll pay you back double when I return."*

Rapid love-bombing + fabricated loss to evoke sympathy and demand money.

Pattern of Investment Scam

Message Hook: *"Hey! I made $10K last week trading crypto—easy method! Join my group for tips. Invest $500 now and double it by Friday. Link: [fake site]."*

Urgency Follow-Up: *"Market crashing soon! Transfer $1,000 to my broker account in the next hour or lose everything. Proof attached—see my profits screenshot."*

Red Flag: Unsolicited "guaranteed" gains + pressure to act fast, leading to fake apps that "show" growth before vanishing funds.

Lexis in Scammer Discourse

In everyday life, it's often the case that individuals with financial resources wield greater influence and authority. However, scammers employ a completely counterintuitive strategy that hinges solely on the manipulation of language. They craft narratives that intentionally depict themselves as powerless.

Frequently, they resort to repeated phrases designed to elicit sympathy and a sense of obligation from their targets, such as, *"I'm helpless," "only you can save me,"* or *"I'm stuck without you."* By doing so, they transform the dynamics of power. The victim, initially perceived as the one in control due to their resources, is subtly shifted into the role of the *"savior."* This shift can evoke feelings of responsibility and strength in the victim, fostering a sense of empowerment that is, in reality, an illusion.

As the victim internalizes this fabricated narrative, they become increasingly invested in the scammer's plight. This misguided sense of agency is a pivotal tactic; while the victim believes they are taking charge and acting heroically, the genuine power—encompassing wealth, security, and decision-making authority—quietly transitions from the victim to the scammer. In this way, the scammer effectively inverts the power dynamic, rendering the victim vulnerable and unwittingly complicit in their own exploitation..

Perspectives on Power and Social Inequality: CDA Approach

As van Dijk (2001) explains, CDA views discourse as a form of social practice that shapes cognition and legitimizes dominance, often through subtle ideological manipulation. Fairclough (2013) extends this with a three-dimensional model: textual analysis (linguistic features), discursive practice (how texts draw on genres), and sociocultural context (broader ideologies like globalization). Wodak's discourse-historical approach (2001) emphasizes argumentative topoi (commonplaces) and historical contexts, revealing how discourse perpetuates exclusion and inequality. In digital spaces, scams exploit these dynamics, inverting apparent power (e.g., scammers as "vulnerable") to mask exploitation rooted in global social inequalities, such as economic disparities between the Global North and South. Below, I analyze the provided scam examples using these perspectives, focusing on how language victimizes people by constructing asymmetrical power and reinforcing inequalities.

Romance Scam Example

Initial: *"Hi beautiful... What's your story?"*

Love: *"I knew you were my soulmate... I love you more than words can say."*

Tragedy/Urgency: *"My wife died... He's sick now and needs $2,000... Wire it?"*

From Fairclough's perspective, textually, this uses possessive pronouns "*my soulmate*" " and hyperboles ("more than words can say") to create intimacy, drawing on romantic genres (discursive practice) like love letters or novels. Socioculturally, it reproduces neoliberal ideologies of individual rescue, where the victim (often from affluent regions) is positioned as a savior, masking the scammer's economic exploitation tied to global inequality. Van Dijk's socio-cognitive view highlights how this manipulates mental models: the "*vulnerable widower"* trope controls the victim's empathy, inverting power— the scammer gains control by appearing powerless, victimizing through emotional dependency. Wodak's approach sees historical topoi of *"family tragedy"* (rooted in colonial narratives of the "needy other") perpetuating inequality, as scammers from disadvantaged contexts exploit Western ideals of romance to extract resources. In digital anonymity, this unequal exchange thrives, disempowering victims by normalizing exploitation as *"love."*

Investment Scam Example

Hook: *"I made $10K... Invest $500 now and double it."*

Urgency: *"Market crashing... Transfer $1,000... or lose everything."*

Fairclough analyzes this textually through imperatives *("invest," "transfer"*) and economic jargon ("market crashing"), mimicking business genres to legitimize fraud. Discursively, it hybridizes sales pitches with urgency, socioculturally reinforcing capitalist ideologies where *"opportunity"* equals wealth, but hides power imbalances favoring scammers in unequal global markets. Van Dijk notes cognitive control via fear-inducing models ("lose everything"), limiting alternatives and empowering the scammer to dictate actions, exacerbating social inequality by targeting the financially vulnerable. Wodak's historical lens reveals topoi of "economic crisis" (echoing past financial scandals), historicizing inequality as scammers from under-resourced areas exploit trust in digital capitalism, victimizing through false empowerment *("you'll double it"*). Digital spaces amplify this, as lack of face-to-face cues enables unchecked power shifts.

Linguistic Features and their Role in Power, Social Inequality, and Victimization in Digital Spaces

Critical Discourse Analysis (CDA) provides a robust framework for dissecting how language in scam messages constructs power asymmetries and perpetuates social inequalities, particularly in digital spaces where anonymity amplifies exploitation. Drawing on Fairclough's (2013) three-dimensional model—textual (linguistic elements), discursive (genre and intertextuality), and sociocultural (ideological contexts)—this analysis reveals how scammers use everyday language to invert power dynamics, positioning victims as "rescuers" while extracting resources. Van Dijk's (2008) socio-cognitive approach emphasizes how discourse manipulates mental models to legitimize dominance, often exploiting global inequalities like economic disparities between the Global North and South. Wodak's (2016) discourse-historical lens highlights argumentative topoi (e.g*., "crisis"* or *"family bond"*) that historicize inequality, drawing on cultural narratives to normalize victimization. In digital realms, these features transform impersonal platforms into sites of ideological control, victimizing users by commodifying trust and empathy amid unequal access to verification tools. In conclusion, linguistic features—urgency, intimacy, and authority—contribute to power by inverting hierarchies and to social inequality by leveraging economic and cultural divides, ultimately victimizing in digital spaces where language fills verification voids. CDA underscores the need for awareness to disrupt these ideologies.

DISCUSSION

The findings highlight how scammer discourse perpetuates significant power imbalances, resonating with the Critical Discourse Analysis (CDA) critique of language as a vehicle for ideology, as articulated by van Dijk in 2008. The concept of "urgency stories" commodifies time, transforming not just financial contributions but also emotional investments, such as love declarations and familial ties—each of these elements becomes intertwined within the framework of neoliberal globalization. By employing virtual ethnography, researchers uncovered subtle nuances and complexities that traditional survey methodologies would likely overlook.

The implications of this research are far-reaching, particularly in enhancing the detection of scams through the identification of specific linguistic markers. Additionally, there is a pressing need for educational initiatives that inform potential victims about the discursive red flags associated with these deceptive narratives. Future research might benefit from a multimodal approach, analyzing the use of emojis or intonations in voice notes, as suggested by Machin and Mayr in 2012.

Scammers often adopt a façade of weakness and desperation, crafting narratives that evoke sympathy by stating things like, "*I'm all alone, and my child is in a critical condition."* This tactic flips the dynamics of power, positioning the victim as the one who feels strong and needed in this pseudo-vulnerable exchange.

Typically, scammers adhere to a fixed script designed to ensnare their targets emotionally. Initially, they inundate the victim with declarations of love, asserting, *"You're my soulmate,"* which establishes a rapid emotional connection. Following this, they unveil a fabricated tragic saga—such as the death of a wife or the illness of a child—designed to tug at heartstrings. The narrative culminates in an urgent plea for financial assistance, often framed as a life-or-death scenario: *"Send money now or she dies!"* This creates a sense of panic that effectively traps individuals emotionally, mirroring the manipulative tactics often employed by abusers in real-life relationships.

Moreover, these scam narratives are often rife with intense emotional expressions but lack concrete details—sights, sounds, smells, or specific locations—leaving them feeling dramatic yet suspiciously hollow. This combination of big feelings and vagueness enhances their manipulative power while raising red flags for discerning individuals..

Limitations

The personas that were adopted played a crucial role in determining the types of scammers who engaged with the researcher, as well as the specific scripts they utilized during their interactions. It was observed that different demographic factors—such as being male, younger, or belonging to a non-Western background—led to variations in the types of scams encountered by victims. This highlights the nuanced approach scammers take in tailoring their methods to exploit particular vulnerabilities.

Furthermore, the emotional labor involved in sustaining affectionate and engaging responses over several months was significant. This ongoing commitment required not just personal resilience but also access to support systems to cope with the emotional toll. Despite the challenges, the researcher achieved an impressive outcome simply by acting as a receptive and actively engaged conversational partner. This approach allowed for the creation of what can be considered the most authentic and sequential record of live scammer discourse available for scholarly analysis. Such a detailed and genuine account provides invaluable insights into the dynamics of online scamming and the psychological interplay between scammers and their victims.

CONCLUSION

The discourse surrounding scams, when examined through the lens of Critical Discourse Analysis (CDA), reveals a range of manipulative strategies that take advantage of inherent human vulnerabilities. This article delves into three specific case studies through the methodology of virtual ethnography, providing a comprehensive analysis of how scammers effectively utilize emotional drivers such as urgency, love, and tragedy. These tactics are critical in deceiving individuals and prompting them to act against their better judgment.

The findings underscore the pressing need for interdisciplinary interventions that can address the complexities of scam operations and their psychological impacts. By fostering a deeper understanding of how these ideologies function, we can better equip potential victims with the knowledge and tools to recognize and resist such manipulative practices. Ultimately, enhancing awareness serves to demystify the mechanisms behind scams, empowering individuals to protect themselves from falling prey to these predatory schemes.

REFERENCE

1. Anafo, C. (2020). On the grammar of scam: Transitivity, manipulation and deception in scam emails. World Englishes, 39(2), 248–262.
2. Boellstorff, T., Nardi, B., Pearce, C., & Taylor, T. L. (2012). Ethnography and virtual worlds: A handbook of method. Princeton University Press.
3. Brown, P., & Levinson, S. C. (1987). Politeness: Some universals in language usage. Cambridge University Press.
4. 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.
5. Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. Security Journal, 27 (1), 36-54.
6. Chilton, P. (2004). Analysing political discourse: Theory and practice. Routledge.
7. Calvey, D. (2017). Covert research: The art, politics and ethics of undercover fieldwork. Sage.
8. Ess, C. (2014). Ethics in internet ethnography. In Handbook of ethnography (pp. 487-503). Sage.
9. Fairclough, N. (2013). Critical discourse analysis: The critical study of language (2nd ed.). Routledge.
10. Federal Trade Commission. (2023). Consumer sentinel network data book 2022. FTC.
11. Hammersley, M., & Atkinson, P. (2007). Ethnography: Principles in practice (3rd ed.). Routledge.
12. Hine, C. (2000). Virtual ethnography. Sage.
13. Lazarus, S. (2018). Birds of a feather flock together: The Nigerian cyber fraudsters (Yahoo Boys) and hip hop artists. Criminology, Criminal Justice, Law & Society, 19 (2), 63-80.
14. Machin, D., & Mayr, A. (2012). How to do critical discourse analysis: A multimodal introduction. Sage.
15. van Dijk, T. A. (2008). Discourse and power. Palgrave Macmillan.
16. Vrij, A., Granhag, P. A., & Porter, S. (2010). Pitfalls and opportunities in nonverbal and verbal lie detection. Psychological Science in the Public Interest, 11 (3), 89–121.
17. Whitty, M. T., & Buchanan, T. (2012). The psychology of the online dating romance scam. University of Leicester.
18. Whitty, M. T., & Buchanan, T. (2016). The online dating romance scam: The psychological impact on victims—both financial and non-financial. Criminology & Criminal Justice, 16 (2), 176–194.
19. Wodak, R., & Meyer, M. (Eds.). (2016). Methods of critical discourse studies (3rd ed.). Sage.
20. Xu, W., Zhang, Y., & Li, Y. (2023). What makes deceptive online reviews? A linguistic analysis perspective. Humanities and Social Sciences Communications, 10, 1–12.