© IIJP 2026 | Volume 2, Issue 3, pp. 1483-1508| ISSN: 2636-4484

A STYLISTIC ANALYSIS OF PHISHING MESSAGES IN NIGERIAN WHATSAPP SCAMS

***Amos Baba Itari[1], Prof. Amodu, Eneojoh Jonah[2] & Prof. Prisca Godspower Ochulor[3]**
[1&3]Department of English and Literary Studies, Bingham University Karu, Nasarawa State, Nigeria
[2]Department of English and Literary Studies, Ahmadu Bello University, Zaria, Kaduna State
***Corresponding Author:** amosbaba777@gmail.com

ARTICLE INFO
Article No.: 0528
Accepted Date: 01/08/2026
Published Date: 29/08/2026
Type: Research

ABSTRACT
This study conducted a stylistic analysis of manipulative language in phishing messages circulated among online fraudsters on WhatsApp in Nigeria. Phishing is one of the most alarming problems in contemporary digital communication, and the evidence for its scale in Nigeria is considerable. The study adopted a qualitative research methodology focusing on content analysis, combining the stylistic model of Leech and Short (2007) with the rhetorical framework adapted by Hoyland (2001). Ten phishing messages collected from WhatsApp between 2022 and 2025 were purposively sampled and analysed for their linguistic and stylistic features. The analysis found that fraudsters draw on carefully selected lexical items from specific semantic fields to create trustworthiness, urgency, and desire. Grammatically, the messages combine declarative statements, imperative commands, strategic tense choices, and deliberate departures from Standard English to compel a response. Rhetorically, the messages employ appeals to ethos, pathos, and logos, often reinforced by figures of speech such as personification, hyperbole, and direct address. The study concludes that online fraudsters function as skilled and ethically corrupt stylists who exploit linguistic convention, symbolism, institutional credibility, and human vulnerability to achieve their fraudulent ends. It is recommended that telecom regulators, cybersecurity educators, and digital literacy programmes draw on these stylistic patterns to strengthen public awareness and improve the detection of WhatsApp-based phishing messages.

Keywords: stylistics, phishing messages, manipulative language, lexical choices, grammatical structures, figures of speech

.

Introduction

Style is the way in which linguistic elements are employed to convey meaning, express identity, or achieve specific communicative objectives, and it involves deliberate choices in vocabulary, sentence structure, tone and rhetorical technique shaped by context, audience and purpose (Hassan, 2021). Beyond registers such as formal, informal, technical or literary, style also functions as a linguistic signature that differentiates one writer from another, encompassing prosodic, visual and structural elements as well as lexical and syntactic choices.

Phishing is a form of online fraud that uses deceptive communication to trick individuals into disclosing sensitive information such as passwords, credit card numbers or personal details. Hashim, et al (2017) noted that phishing communications often manipulate language to appear authoritative, using fear, curiosity or authority to elicit a desired response, and such stylistic cues contribute to the urgency, credibility and persuasiveness of phishing messages, making them effective tools for deception (Hua, Abdollahi-Guilani, & Zi, 2017). A thorough understanding of these stylistic techniques can help counteract such threats and strengthen protections for individuals and organisations (Taylor, 2019). In Nigeria, this threat increasingly circulates through WhatsApp rather than email, and it is on the stylistic features of these Nigerian WhatsApp phishing messages that the present study concentrates.

Accordingly, this study performed a stylistic analysis of online scam messages, as evidenced by phishing messages, using the Stylistic Framework by Leech & Short and Rhetoric as its theoretical framework.

Phishing has become one of the most alarming problems in contemporary digital communication, and the evidence for its scale in Nigeria is now considerable: Ashiru (2021) identifies it as a distinct form of cybercrime within the Nigerian legal and social environment, and the Daily Independent (2026) reports that Nigeria is the most spammed country in Africa. However, existing studies of Nigerian phishing concentrate largely on email and advanced-fee fraud, are predominantly pragmatic, discursive or forensic in orientation rather than systematically stylistic, and rarely integrate the description of linguistic form with an account of persuasive effect; in particular, the way fraudsters combine stylistic choices with rhetorical appeals (ethos, pathos, logos) in the WhatsApp messages that now reach the greatest number of Nigerian users has not been documented. This gap matters because, where the linguistic mechanisms of deception remain undescribed, awareness campaigns and detection systems are left to rely on surface indicators such as spelling errors, which the more sophisticated messages examined in this study no longer display. This study therefore fills that gap by providing a combined stylistic and rhetorical analysis of Nigerian WhatsApp phishing messages.

Several strands of literature inform this study. Reviews of the field by Adu-Manu, Ahiable, Appati and Mensah (2022) and by Olasehinde (2024) show that phishing has continued to evolve in tactics and in reach, moving from electronic mail into mobile and social messaging platforms. What is significant for the present study is that the success of these attacks does not rest on technical intrusion: Desolda, Ferro, Marrella, Catarci and Costabile (2021), in a systematic review of human factors in phishing, demonstrate that the decisive moment is the recipient's response rather than any breach of a system, and Carter (2023) shows that fraudsters compel compliance through carefully managed language rather than through force. Xu and Rajivan (2023) similarly establish that the psycholinguistic properties of a message contribute measurably to its deceptive power. Phishing is therefore, in the first instance, a linguistic problem, and it is on the language of these messages that the present study concentrates.

Several gaps and inconsistencies nevertheless remain in this body of work. In the first place, the Nigerian studies concentrate largely on electronic mail and on advanced fee fraud, whereas the messages that now reach the greatest number of Nigerians circulate through instant messaging platforms, a shift acknowledged by Ahmad, Terzis and Renaud (2024) but not yet examined stylistically in the Nigerian setting. Secondly, the available analyses are predominantly pragmatic, discursive or forensic in orientation, so that they identify strategies of deception or attempt authorship attribution without applying a comprehensive stylistic checklist of the kind proposed by Leech and Short (2007) across the lexical, grammatical, figurative and contextual categories. Thirdly, and most importantly for the present research, the literature divides between studies that describe linguistic form and studies that describe persuasive effect, with very few attempting to integrate the two, so that descriptions of style are frequently offered without an account of why the features described actually persuade, while accounts of persuasion are offered without being anchored in verifiable textual evidence. Finally, the recent Nigerian pattern in which fraudsters impersonate federal agencies, telecommunication brands, religious appeals and celebrity events has not been documented in a single sustained corpus, so that the ways in which stylistic choices are adjusted across successive versions of the same campaign remain largely unrecorded.

These gaps matter because the consequences of the problem are severe and well documented. Whitty (2024) shows that the harm suffered by victims of online fraud extends well beyond financial loss to psychological and social damage, and Jolaiya (2024) records the effect of electronic fraud on financial confidence. The present research therefore undertakes a stylistic study of phishing messages circulating among Nigerian users, combining the stylistic model of Leech and Short (2007) with the rhetorical framework adapted by Hoyland (2001), in order to describe the linguistic resources through which these messages are constructed and to explain the persuasive work that those resources perform. In doing so, the study responds directly to the gaps identified above and provides an evidential basis for awareness, detection and prevention.

Aim and Objectives of the Study

The primary objective of this study was to conduct a stylistic analysis of manipulative language in phishing messages from online fraudsters. The specific objectives of the study are to:

1. analyse the lexical choices employed by scammers in phishing messages;
2. examine the grammatical structures employed in phishing messages;
3. identify the use of figures of speech in phishing messages;
4. examine the rhetorical appeals (ethos, pathos and logos) used in phishing messages.

Research Questions

The study was guided by the following research questions:

1. What lexical choices are employed by scammers in phishing messages?
2. What grammatical structures are employed in phishing messages?
3. How are figures of speech used in phishing messages?
4. What rhetorical appeals (ethos, pathos and logos) are used in phishing messages?

Theoretical Framework

Two theories underlie the study: the stylistic approach developed by Leech and Short (2007), and the theory of rhetoric attributed to Aristotle, as cited in Hoyland (2001). Neither theory alone is sufficient for the present investigation. The stylistic approach is highly efficient in analysing the linguistic devices used for foregrounding and the formation of meaning, but it does not provide a systematic account of why these devices persuade or influence readers' decisions, since it offers no way to analyse appeals to ethos, pathos and logos. Conversely, the

theory of rhetoric (Aristotle, as cited in Hoyland 2001) allows a thorough analysis of persuasive appeals, but it does not provide the set of lexical, grammatical and stylistic categories needed to describe deceptive texts such as phishing messages. The researcher therefore combined both theories, adapting only the checklist criteria relevant to this study — lexical, grammatical, figures of speech and foregrounding from the stylistic approach, and ethos, pathos and logos from rhetoric — while setting aside more abstract matters such as the "philological circle."

Stylistic Framework by Leech and Short (2007)

This research adopted the stylistic approach developed by Leech and Short. In order to accommodate the grammatical, lexical, and rhetorical features of speech and foregrounding in the selected messages. The stylistic approach developed by Geoffrey Leech and Mick Short first appeared in 1981 and was revised, enlarged, and republished in 2007. The approach asserts that style is about the linguistic characteristics of a specific text, while stylistics is concerned with explaining why certain linguistic choices have been made and their impact on communication or art. Therefore, stylistics deals with the relationship between the form and the meaning in terms of language by considering the text as the primary source of evidence. Leech and Short claim that stylistic analysis becomes productive only if it operates between descriptive linguistic analysis and interpretative insights through a "philological circle," whereby observations of the text inform interpretations, and the latter direct the former observations. This approach is concerned with understanding how linguistic features contribute to creating meaning in the text, whether the meaning is characterised by characterisation, persuasion, humor, emotion or deception in the case of deceptive texts. This stylistic approach is especially helpful in analysing phishing texts, as these texts are deliberately designed to deceive recipients. Based on the provided checklist, the analysis can start by examining the lexical categories, in which the fraudulent sender uses formal, urgent, and authoritative language, along with institutional names and emotional triggers, to lend legitimacy to their claims and create a sense of urgency. The grammatical categories enable one to see how imperative verbs, commands, tense selection, voice and sentence adverbs build up the pressure of what is being conveyed through the message. The category of figures of speech accounts for the metaphor, hyperbole, personification, direct address and repetition through which the message magnifies the threats and the potential benefits and gives an abstract institution the appearance of human generosity.

Rhetoric

The above discussion on rhetoric theory shows that this study relies on Carl Hoyland's (2001) adaptation of Aristotle's rhetorical theory. The reason is that fraudulent schemes usually rely on establishing a fictitious sense of credibility (ethos), triggering emotions such as fear, hope or urgency (pathos), and presenting apparently logical reasons for taking a particular action (logos). Consequently, this research was based on both the stylistic model of Leech and Short (2007) and rhetoric theory as adapted by Hoyland (2001). The rationale for this decision is that neither theory, taken by itself, would be sufficient to address the objectives set for the research. A stylistic approach enabled the researcher to investigate the lexical, grammatical, figurative and contextual elements found in the phishing messages, together with the foregrounding and deviation through which those elements are made prominent or concealed. Rhetoric theory enabled the researcher to account for the persuasive techniques by which those same elements act upon the recipient.

Methodology

The study adopted a qualitative research methodology focusing on content analysis. The main data source was phishing messages collected from the WhatsApp platform. The study

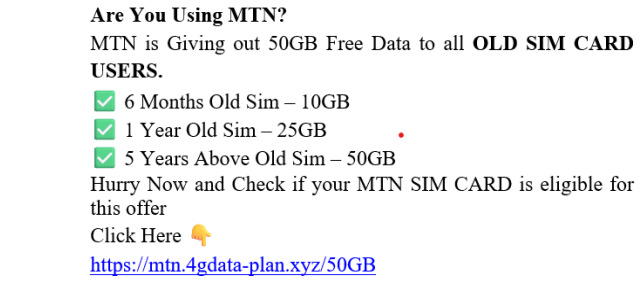
utilised a purposive sampling strategy, which involved the purposeful selection of data based on specific criteria relevant to the research questions posed. In this particular case, the selected data, spanning 2022-2025, consisted of 10 phishing messages showing linguistic and stylistic features of fraud, such as persuasion techniques, emotionality, a false sense of urgency, impersonation or atypical format. Each message was verified using checkphish.ai to confirm that it was phishing rather than legitimate before being included in the corpus. Ten messages were judged sufficient for this qualitative, purposive sample because they were selected to represent the range of scam types (government, corporate, religious, celebrity, educational and poverty-alleviation) circulating on WhatsApp during the period, and analysis of the set reached a point of data saturation, at which additional messages of the same type were no longer yielding new stylistic or rhetorical categories. Because the data consisted of other people's private WhatsApp messages, ethical care was taken in handling them: no real names, phone numbers or other victim-identifying details are reproduced in this study, and every message is discussed solely for its linguistic and stylistic features rather than to identify or expose any individual. The data analysis method for the study is based on a combination of the stylistic approach of Leech and Short (2007) and the adapted Aristotelian rhetoric of Carl Hoyland (2001), applied through thematic content analysis. The stylistic approach served as the tool for the in-depth linguistic analysis of the phishing messages, using the adapted checklist of lexical categories, grammatical categories, figures of speech and context set out by Leech and Short (2007). The deficiency of relying solely on a stylistic approach is that it fails to provide an in-depth analysis of the persuasive nature of these linguistic categories, which is why the rhetorical framework of ethos, pathos and logos was combined with it.

Results and Discussion

This chapter presents and analyses the ten phishing messages described in the Methodology, examining each in turn for its lexical, grammatical and rhetorical features. It also includes the research's general findings, how they compare with other authors' work, and how the applied theories relate to the findings. The ten messages presented below were chosen because, together, they represent the main scam types identified on WhatsApp during the sampling period — government impersonation, corporate brand hijacking, religious appeal, celebrity association, educational opportunity and poverty-alleviation schemes — so that the analysis captures the stylistic range of the wider set of messages collected rather than a single scam type.

Datum 1

Datum 1


Are You Using MTN?
MTN is Giving out 50GB Free Data to all **OLD SIM CARD USERS.**
✅ 6 Months Old Sim – 10GB
✅ 1 Year Old Sim – 25GB
✅ 5 Years Above Old Sim – 50GB
Hurry Now and Check if your MTN SIM CARD is eligible for this offer
Click Here 👇
https://mtn.4gdata-plan.xyz/50GB

The words are placed in the sphere of telecommunications, promotion and rewards. The mention of the known company adds a sense of officiality to the whole text: "MTN," "SIM CARD," "Data Plan." The name of the program, "50GB Free Data," is catchy and alluring. The words "50GB Free Data" involve the ideas of value ("FREE," "Giving out"), technology ("Data," "GB") and personal relation ("OLD SIM CARD," "eligible"). The time frames and figures seem to be

carefully selected: "50GB," "6 Months," "1 Year," "5 Years," etc. The words which describe the offer look like they were especially selected in order to cause an emotional response from the reader. "Hurry Now," "Check if your... is eligible" look like there is something exclusive and limited-time offer for the reader. There are the action verbs "Click Here," "Hurry Now," "Check" used in order to limit the choice of the reader. The repeated "Old SIM CARD" personalises the message. There is also use of simple language that has no technical terms whatsoever, thus making it easy for the readers to understand what the text says. In this way, scammers use their words to gain the confidence of their victims, make them think faster, and manipulate the psychological behaviour of the reader.

As far as grammar goes, the whole text is made up of short and directive sentences. The headline of the scamming text is the direct question: "Are you using MTN?" This question creates a conversation with the reader making him/her interested enough to continue reading the text. Following the question is a declarative sentence that says: "MTN is Giving out 50GB Free Data to all OLD SIM CARD USERS." Present continuous is used in order to show immediacy: "is Giving out". It is typical for advertising of some current promotion campaigns. The body of the text is comprised of noun phrases separated with dashes: "✓ 6 Months Old Sim -- 10GB," and so on. This is not an ordinary sentence; rather it is a kind of shorthand that is used in promotions. The message contains imperatives: "Hurry Now," "Check," and "Click Here." The imperative voice in this message is very strong, leaving no place for any politeness. The final part of this message, the URL, is one noun phrase serving as a call-to-action element. All verbs in this text are written in the active voice: "MTN is Giving out" and "Click Here." In this way, readers feel their strength and power, and they can be compared to passive voice messages in more formal texts. There are no long and complicated sentences in the whole message; this text is very clear and straightforward. This message is written in the second person singular perspective, using pronouns like "you" and "your." In this way, the message gets personal touch, together with other grammatical tricks that help to take away nuance, make people act faster and show the use of simple language by scammers.

The phishing message tries to influence the reader, pretending to be a corporate message. This is the authoritative (ethos) phishing message since it makes a reader believe in the legitimacy of the message through the mention of well-known company and its corporate identity. Copying of the corporate language occurs through mentioning the product ("Data," "GB"), the offer ("Free Data") and the structure of a promotion. A causation is present in the message in the implication that loyal clients (people who have an old SIM card) should be offered a reward. Being "eligible" for anything under certain conditions ("6 Months Old Sim") is an attempt to play upon the emotions (the need for a reward) and the logic (it's a fair process). "Hurry Now" is the pressure applied by the message, instilling fear of losing the opportunity. It is important that although the message does not specifically ask to do anything, the feeling of personal benefit encourages the recipient of the message to respond immediately without thinking about it. This message seems to be a corporate promotional message, and it consists of a standard structure: identification of the target group (old SIM card owners), presentation of the offer, provision of a simple way to determine if one is eligible for the offer and a straightforward call to action. All of this adds up to a believable and generous corporate initiative, leveraging trust in a familiar brand and the desire for a good deal to carry out this fraud.

Datum 2



The lexical structure of this phishing message is designed to exploit particular cultural, religious and socioeconomic semantic fields and develop a compelling discourse of holy charity, communal duty and lucrative opportunity. The lexicon is deliberately split into two sections, mirroring the code-switching evident in the graphological layout, each section of each language serving different but complementary manipulative purposes. The English-language title is designed to convey the underlying fraudulent message using a lexicon selected for maximum impact and credibility. “ALHAJI AMINU DANTATA” is not merely a name but a word-group carrying associations of vast wealth, business acumen, Islamic devotion (with “Alhaji” as a title) and Northern Nigerian heritage. “WEALTH DISTRIBUTION” is a highly effective word group, semantically framing this action as a systematic, possibly obligatory distribution of wealth, reminiscent of Zakat (Islamic almsgiving) or family inheritance. The specific figure of “N20,000” is used for lexical precision, making this offer more concrete and believable than vague promises. The Hausa text similarly employs a word-group deeply embedded in religious and communal culture, thereby being central to its emotional and ethical appeal. Some of its key words include:

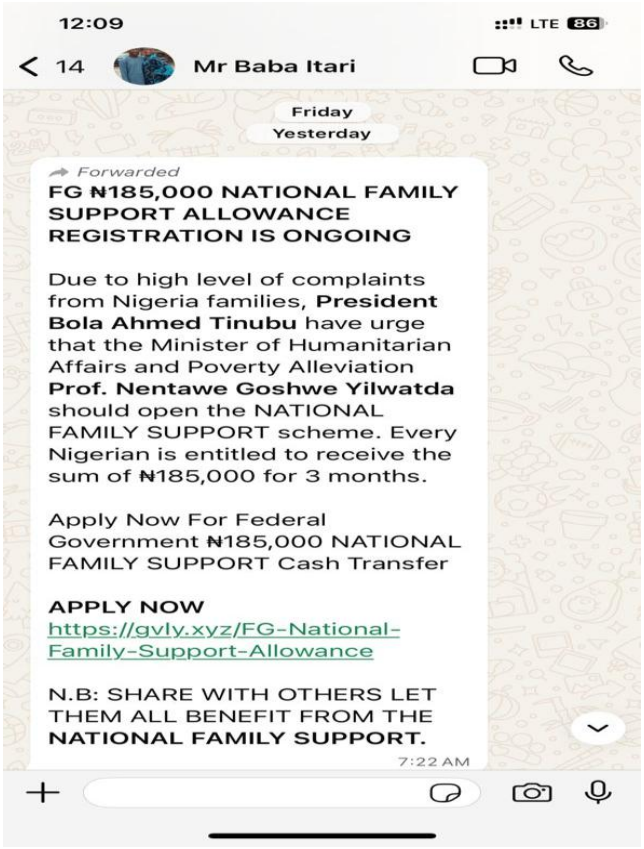
1. Tallafi: This term refers to "assistance" or "aid," especially charitable assistance.
2. Marasa karfi: This term refers to "the less powerful," "the vulnerable," or "the needy."
3. Ubangiji: This term refers to "The Lord (God)."

A grammatical analysis of the phishing message reveals a syntactic structure that resembles a rhetorical shift from formal announcement to direct instruction, using simplicity, declarative authority and imperative force to achieve the objective. The grammar is designed to facilitate code-switching and the presentation of the scam as a legitimate announcement. The message begins with a noun phrase headline acting as a title: "ALHAJI AMINU DANTATA

N20,000 WEALTH DISTRIBUTION." It is not a sentence but a grammatically highlighted headline typical of announcements and titles. It instantly introduces the theme with authoritative emphasis. The next Hausa text is a complex sentence of the declarative kind: "*Tallafi ne daga gidauniyar marigayi Dantata na kudi N20,000 ga marasa karfi don yi masa addu'ar dacewa a wajen ubangiji*." Grammatically, the sentence is complex. It uses the copula verb "ne" for definition ("*Tallafi ne*" – "It is assistance"), preposition phrases ("*daga gidauniyar*" – "from the foundation of") and a purpose clause using "don" ("*don yi masa*..." – "in order to perform for him..."). This grammatical complexity is typical of Hausa and expresses the seriousness, formality and logic of the transaction (help for prayers). This is in stark contrast to the telegraphic style of Datum 1, where grammar is adapted to fit the formality of the culturally specific announcement. The change to English for the instructions is a shift towards simpler, more direct language. The sentence "Zaku iya neman wannan tallafi da aka fara bawa alumma." ("You can request this assistance that has started being given to the public.") is a declarative sentence using the modal verb "iya" (can) for possibility. The sentence is soft and invites action. Immediately after, there is a blunt imperative: "Shiga yanzu don tura Account Number 👇". This sentence is grammatically very simple: an imperative verb ("Shiga" – Enter/Join), a time adverb ("yanzu" – now), a purpose word ("don" – to) and an infinitive verb ("tura Account Number" – submit account number).

This culturally-targeted phishing message uses a wide variety of rhetorical devices that target particular religious and social values. At its heart is the use of false ethos, where the scammer attempts to leverage the name and reputation of Alhaji Aminu Dantata, a man associated with wealth, business and religious values. He uses this pre-existing association and the idea of a charitable foundation (gidauniyar marigayi Dantata) to give the scam a veneer of legitimacy and moral rightness. Code-switching is a powerful rhetorical device in this scam, not only because it indicates the scammer is part of the target's culture and thus has a deeper emotional connection to the target, but also because it adds a veneer of authenticity. At its heart is a spiritual transactional framework, in which the offer is not given in return for nothing but for the target's prayers (don yi masa addu'ar dacewa). This scam appears to be a good exchange that is religiously reasonable. It appeals to the reader's religiosity and desire to earn merits (pathos). It uses more emotional appeals (pathos) to evoke the reader's sympathy for people in need (marasa karfi) and to encourage them to assist the community. It employs a false sense of urgency (chronos) through commands such as "Shiga yanzu" (Enter now), which encourage people to act immediately. It assumes a style similar to that of a real charity or religious notice to gain the reader's trust. In total, it crafts a false narrative that leverages cultural and religious sentiments to perpetrate a highly harmful, believable scam.

Datum 3



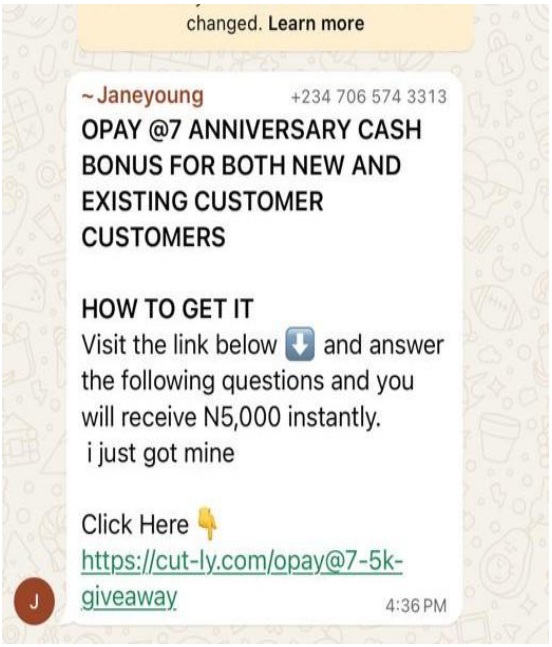
The words place themselves within the domain of government, policy and welfare states. The use of abbreviations gives an air of bureaucratic authenticity: "**FG**" for Federal Government, "**N.B.**" for Nota Bene. The name for the programme, "**NATIONAL FAMILY SUPPORT ALLOWANCE**," is a good, strong choice. It uses big words associated with nation-states ("NATIONAL," "FAMILY"), good policy words ("SUPPORT") and a good financial word ("ALLOWANCE"), similar to words used for actual programmes: "Conditional Cash Transfer" or "National Social Safety Net." The numbers and dates look like they were deliberately chosen. "**₦185,000**" is not a round number. "**For 3 months**" sounds plausible. The words used to describe the complaint and response seem chosen deliberately. "**Due to the high level of complaints from Nigerian families**" sounds like they care about their people. "**Have urge**" is not correct grammar. It is trying to sound like government speech. "**Should open**" sounds like they have been too busy to open it. The titles look official. "**President Bola Ahmed Tinubu**" is a real president. "**Minister of Humanitarian Affairs and Poverty Alleviation Prof. Nentawe Goshwe Yilwatda**" sounds real, too. "Humanitarian Affairs and Poverty Alleviation" is the real name of a department in the government. The name of the minister sounds fake because "Yilwatda" sounds too regional. This scam sounds official because it uses official titles. The action words are direct. "**Apply Now For…**", "**APPLY NOW**", "Apply" are action words. "Apply" sounds official and is intended for use in a government program. "**SHARE WITH OTHERS**" talks about sharing and gaining. "**LET THEM ALL BENEFIT**" talks about everyone. It is an official speech. It is direct. It uses long words. It uses official speech. It talks about "Registration is ongoing" and "is entitled to receive." It sounds official. It does not use casual words like "free," "hurry," or emojis. It is trying to sound official. However, there are

minor grammatical errors in the text, such as the use of the word "have urge" and "gvly.xyz." These are uncommon words and look unusual as a domain name.

In terms of grammar, the text has a headline consisting of a noun phrase and a verb phrase: "FG №185,000 NATIONAL FAMILY SUPPORT ALLOWANCE REGISTRATION IS ONGOING." The use of "Registration is ongoing" is the present continuous tense, which is commonly used in official announcements such as "Enrolment is open" or "Distribution is underway." In terms of grammar, the text uses complex sentences. The first sentence, "Due to a high level of complaints from Nigerian families, President Bola Ahmed Tinubu has urged that the Minister... should open the NATIONAL FAMILY SUPPORT scheme," has features of Nigerian official writing or translated texts. The use of the phrase "high level of complaints" is a complex noun phrase and sounds formal. The use of the verb phrase "have urge" is not standard English; however, the minor grammatical error sounds more natural to readers of local official communications. Moreover, the use of the phrase "should open" after the word "urge that" uses the subjunctive mood, which sounds formal. The second sentence reads: "Every Nigerian is entitled to receive the sum of ₦185,000 for 3 months." This is clear and strong. The use of the present simple verb "is entitled to receive" is used to state a general truth. The passive voice of "is entitled to receive" makes it more objective, as is expected in a government program. The addition of "for 3 months" states the time frame. The imperative: "Apply Now For Federal Government ₦185,000 NATIONAL FAMILY SUPPORT Cash Transfer." This is not a sentence but a command in the imperative voice, used for emphasis. The phrase "**APPLY NOW**" is a command. The use of the imperative voice, in both paragraphs, changes from a command to a direct action. This could be a demonstration of a government programme represented online, with a command followed by an action. The last line: "N.B: SHARE WITH OTHERS, LET THEM ALL BENEFIT FROM THE NATIONAL FAMILY SUPPORT." This is a mix of the imperative "SHARE WITH OTHERS" and a purpose clause "LET THEM ALL BENEFIT." The use of the imperative "LET THEM ALL BENEFIT" to state a suggestion is typical of advisory writing.

This phishing message pretends to be from the government by mimicking government-speak. It is an authoritative idea (ethos) phishing message because it makes the reader believe it is real by mentioning the name of the President of Nigeria, Bola Tinubu and a minister of the Ministry of Humanitarian Affairs, Prof. Nentawe Goshwe Yilwatda. It pretends to be from the government to prevent the reader from becoming suspicious. It is copying the government's language by mentioning the programme's name, “FG,” the budget and the language. A false cause-and-effect statement is the opening statement of the message. It tells the reader that the government is addressing people's complaints by providing the program. The idea of everyone being entitled to something is a mix of emotional appeal (concern for money) and a claim of a legal right. “REGISTRATION IS ONGOING” is the urgency of the message. The key point is that the text "**N.B: SHARE WITH OTHERS LET THEM ALL BENEFIT**" is using social proof and makes the reader want to help. It makes the reader become a "spreader" for viral propagation. The text appears to be a Public Service Announcement (PSA) and follows this structure: it identifies a need, outlines government action and instructs citizens on how they can help. It also instructs the reader to share it. All of this makes it easy for the reader to read and process on a superficial level, but not critically. All of this adds up to a believable and caring government initiative, leveraging trust in authority and communal obligation to carry out this fraud.

Datum 4



The most notable graphical element is the large, unspaced header: "OPAY @7 ANNIVERSARY CASH BONUS FOR BOTH NEW AND EXISTING CUSTOMERS." The logo "OPAY," the event "@7ANNIVERSARY," and the keywords "CASH BONUS" and "CUSTOMERS" are intended for quick recognition, connecting the message to a fintech company's celebratory giveaway. The repetition of "CUSTOMERCUSTOMERS" appears to be a rushed or hurried creation, a slight error that may be overlooked in the excitement of the offer. The body of the message employs brief, direct lines of text. "HOWTOGETIT" has the same unspaced, headline appearance as a sub-header. The text reads, "Visit the link below / and answer / the following questions and you / will receiveN5,0o0instantly." The text includes intentional spacing errors in words such as "the link below," "the following questions and you," and a spelling error in "N5,0o0" where "o" replaces a "0." The small graphological errors serve two purposes: they resemble the kinds of mistakes one might make in a hurry online, so they do not appear to be "solicitation spam," and the degree of error may filter out those who are not paying close enough attention. The text "i just got mine" is written in lowercase letters without punctuation, which mimics a peer's rapid endorsement to provide a sense of social validation directly within the text. The call to action, "Click Here," stands by itself on its own line. The Word "Click" and "Here" together, along with the capitalisation of the C and the H, make this appear to be a button. Immediately following this is the link: "https://cut-ly.com/opay@7-5k-giveaway." The URL is a graphological feature of interest. The use of "cut-ly.com" instead of a legitimate company website, such as "opay.com" or "opayweb.com" which a company like OPay might use to promote a contest, is a major red flag. The "@7-5k" part of the URL keeps with the promotional theme but shifts away from a website structure. The timestamp "4:36PM" at the bottom of the message adds a touch of meta-graphology, evoking the idea of time, making this message appear to be a recent, specific message in a chat.

OPay is the leading digital money brand in Nigeria. Starting with the brand name establishes trust. Using the word "ANNIVERSARY" conveys a sense of celebration and tradition and signals a special time to thank customers, making the corporate giveaway more credible. For the main offer, the company has chosen "CASH BONUS". Using cash is always

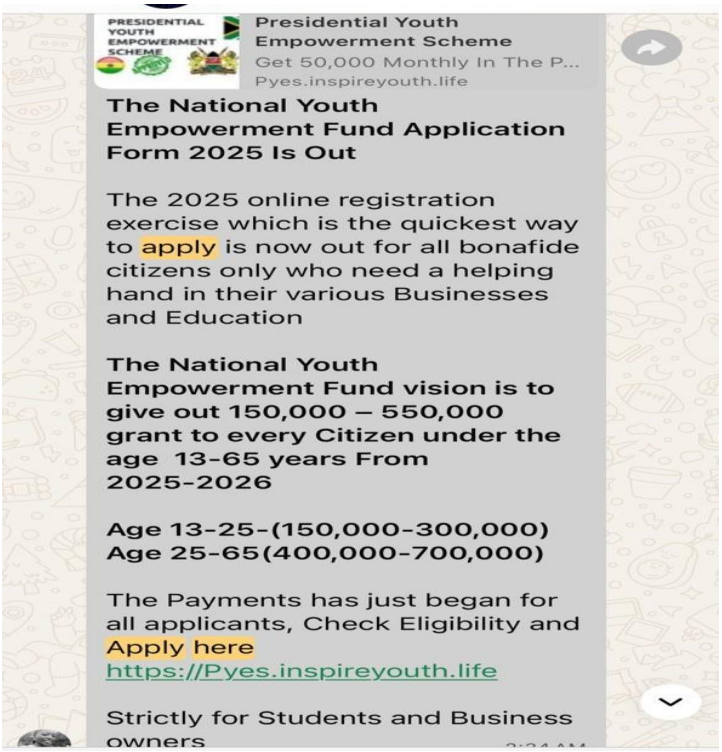
appreciated and a bonus is always good and additional. “FOR BOTH NEW AND EXISTING CUSTOMERS” ensures everyone is included and does not miss out. In the instruction section, the language is extremely simple and clear. Using the word “HOWTOGETIT” makes it sound easy. Visit, answer and receive is a simple three-step process requiring minimal effort. Using the phrase the following questions makes it sound like a simple quiz, not a difficult application. The payoff is promised that you will receive N5,0o0 instantly. Using the word will makes it sound certain. However, the word "will" is used in a sense of certainty rather than possibility. The adverb "instantly" is a key word because it conveys the desire for instant results and eliminates the idea of waiting or checking first. The misspelt word "N5,0o0" is a spelling and letter error. Nonetheless, the actual number "5,000" is clearly spelt out and keeps the offer attractive. The best part is the use of the testimonial "i just got mine." This four-word phrase is a clever use of the English language. It uses the first-person pronoun "I," the past-tense verb "got," and the word "just" to indicate the time factor. It is a clever imitation of a satisfied customer talking. It answers the unstated query "Is this real?" with a believable "I" statement that reduces scepticism significantly. The command "Click Here" is the main command word. It is a common command word used in virtual space. It is easy to understand and requires no further thinking. The other words in the URL ("cut-ly," "giveaway") reinforce the idea of making things easier ("cut" means "shorten" or "easy") and of receiving a prize ("giveaway"). However, the domain "cut-ly.com" is unfamiliar to the OPay brand and disrupts the smooth fintech promo style.

It begins with a phrase, not a sentence, like "OPAY @7 ANNIVERSARY CASH BONUS FOR BOTH NEW AND EXISTING CUSTOMERS." There's no verb and no linking words. It juxtaposes two ideas. This looks like the start of a headline, tag, or message title. It indicates this is not a dialogue but an announcement. The Word "CUSTOMER" is repeated. It is a tiny error, but it is a common mistake, especially when in a hurry or using technology to write. The phrase "HOW TO GET IT" is a noun phrase, again without a verb or command and it serves as a subtitle. It signals a change in tone, from what's being offered to how to obtain it. It is a list of commands and a promise, but it is split into lines: "Visit the link below / and answer / the following questions and you / will receive N5,000 instantly." If you visit the link below and answer the questions, you will receive N5,000 instantly. The punctuation of the lines creates a quick, rhythmic effect, making it easy to read. The lack of space between "the link below" and "the following questions and you" creates a rough feel. The section "you will receive N5,000 instantly" is a simple sentence. Using "will receive" makes it sound incredibly certain, which is a common strategy. The section "i just got mine" is a simple sentence on its own. It is inserted between the command and the action to make it sound like a comment from a different user. The last one, "Click Here," is a sentence with only a verb and an adverb. It has no object because "Here" refers to the link that follows. This is the main thing the message is asking you to do. "4:36 PM" is a noun phrase that gives you the time.

This is a phishing message designed to trick victims. It is using greed or pressure as its mechanism. It claims to come from a legitimate fintech company called OPAY and has the theme of “ANNIVERSARY.” It has a false story of achievement with the phrase “i just got mine.” It promises a quick result with the phrases “answer the following questions” and “will receive…instantly.” It has a command tone with the words “Visit,” “answer,” and “Click.” It is extremely authoritative and you wouldn’t suspect anything. It has a game or quiz theme that is familiar, safe and could even be fun. The key thing is that the sender is using paralipsis because they never tell you what the questions are or what information is required. The short URL "cut-

ly.com" makes everything seem easy, but it is actually not. This tight, focused language tricks you into agreeing without thinking, using trust, proof and promises to secure quick agreement.

Datum 5



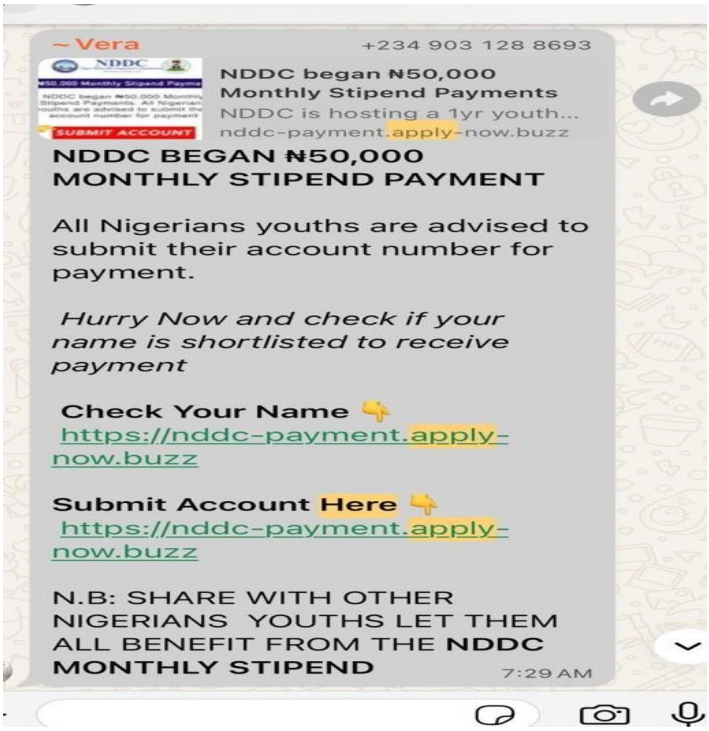
The sender is carefully choosing each word to sound official, trustworthy and inspiring. It remains within the realm of ideas common to government programmes on youth empowerment. It is using official-sounding terms such as "Presidential Youth Empowerment Scheme," "National Youth Empowerment Fund," "Application Form," "online registration exercise," "bona fide citizens," etc. It is a mix of terms that sound very official, which is what a phishing message aims to do. Emotionally uplifting terms are being used, such as "Empowerment," "helping hand," "grant," "Strictly for Students and Business owners." It is trying to evoke an emotional feeling, such as hopes of gaining money, or a desire to get out of a financial bind, which is a common way to persuade, or pathos. Specific terms such as "50,000 Monthly," "150,000 - 550,000 Grant," "13-65 years," and "2025-2026" are used to create a sense of openness, a common phishing tactic to eliminate doubt. Words used in "the quickest way to apply" are associated with efficiency and ease, while "bona fide citizens only" is used to create a sense of special access and eligibility. This is creating a sense of desire and urgency. The repetition of time-related words, "2025," "2025-2026," and "now," is used to create a sense of urgency. The word "grant" is used instead of "loan" to avoid any obligation to pay off, making it sound more attractive. The sentence "The Payments have just begun" creates a sense of progress and a successful start, despite grammatical errors, making it sound active and realistic.

The language used in the phishing message is simple to make it official-sounding. The message presents a false offer as fact, attempting to influence the recipient's action. The message also employs strong statements, such as “The National Youth Empowerment Fund Application Form 2025 Is Out” and “The 2025 online registration exercise… is now out.” The message uses the present tense to indicate that the offer is available at this time. The statements appear to be false announcements, mimicking official press releases to make them seem credible, as they

sound familiar. The message employs the passive voice, as shown in “The Payments have just begun for all applicants.” Despite the subject-verb agreement error, the message presents the payment process as ongoing, which sounds official because it lacks a subject.

It has many tricks that make it believable and help build trust in the organisation. It uses emotions, both old and new, in its message. It gives the fund human qualities by saying, "The National Youth Empowerment Fund vision is to give out," which gives it the qualities of kindness and caring. It uses exaggeration in its message by offering a wide range of grants: "150,000 – 550,000." It also exaggerates the age range of applicants to "13-65 years." This wide range of people is intended to include almost everyone in the country. The large offer is intended to push people into overlooking their doubts. It addresses the reader as "Citizens," "applicants," and "Students and Business owners." This is intended to make the reader feel part of a group that will benefit from the fund. The term "helping hand" is a placeholder for money help. It is a representation of charity and government benevolence, but this benevolence is a disguise for the fact that the message is a scam. It is a scam because of the false credibility, the use of government-sounding big words and the attempt to make the sender sound like a real person in charge of policy. It uses human nature: people want to be financially secure, learn more and own a business. It is using this to lure people in and make them think less clearly. It is using a sense of urgency, using words like "now out" and "has just begun," to make the reader feel like they need to take action before they can check it out. It is using a sense of exclusivity, using phrases like "bonafide citizens only" and "Strictly for Students and Business owners," to make the reader feel special and to make them think this is a legitimate offer. All of this shows the classic techniques of persuasion.

Datum 6



At the graphological level, the message features bold text in capital letters, as seen in the heading "**NDDC BEGAN ₦50,000 MONTHLY STIPEND PAYMENT**". The header also contains the profile name "~ Vera" and the phone number "+234 903 128 8693," which are intended to mimic the sharing of messages on social platforms to make the message seem like it was shared by an

individual, not a phishing attempt. There is also a button labelled "SUBMIT ACCOUNT", which attempts to mimic the interface of legitimate online platforms to make the message seem familiar. The bullet-point format, an asterisk and “Hurry Now and check if your name is shortlisted to receive payment,” using italics and indentation to create a sense of urgency, yet keeping the text visually appealing to capture your interest. The links are shown as “**Check Your Name**” and “**Submit Account Here**.” Below each is the URL, which is “https://nddc-payment.apply-now.buzz”. However, this is not a legitimate government URL, which should end in “gov.ng”. It is a small error that may go unnoticed by someone too engrossed in the visual appeal of the text. It also has a small variation in the second URL, “nddc-payments.apply-now.buzz” from “nddc-payment.apply-now.buzz.” It is a typographical error, but it may also be a deliberate attempt to evade spam filters. It is meant to capture a reader's eye and they may not even notice the error. The final sentence, “N.B: SHARE WITH OTHER NIGERIAN YOUTHS LET THEM ALL BENEFIT,” uses the abbreviation for notation, “N.B.,” and capital letters to make it stand out and then goes on to ask you to share this with others.

The phishing message uses the theme of authority, the need for money and helping the community. This is a clever fraud because it uses specific words from various areas of interest. It uses words such as "NDDC," "Monthly Stipend Payments," "shortlisted," and "payment." These words associate the message with the government and social plans. It uses the trusted image of the Niger Delta Development Commission to sound legitimate. The message "NDDC began ₦50,000 Monthly Stipend Payments" uses the past tense "began" to indicate that the payments have already started. This makes the reader think the plan is already in place and eliminates doubts because it is already underway. There are many urgent and emotional words, such as "Hurry Now," "check if your name is shortlisted," "SUBMIT ACCOUNT," etc. These words evoke a sense of waiting, fear of missing out and hope of receiving money, which relates to the concept of persuasion through emotion (pathos). The word "shortlisted" is a good choice because it implies a real process that you might have succeeded in, which evokes a sense of being complimented based on your merit, so you feel compelled to act fast. Mentioning specific amounts of money, "₦50,000 MONTHLY," "1yr youth," etc., creates a sense of precision and clarity, which is a phishing trick to appear credible by being well-organised. The words "All Nigerians youths are advised" are official words used in government advertisements. The word "Nigerian youths" (even though it is not grammatically correct) includes everyone, making the message reach a wider audience. The word "SUBMIT ACCOUNT" is written in capital letters to encourage immediate action. The word "SHARE WITH OTHER NIGERIAN YOUTHS" utilises words that help the community, encouraging people to share with other Nigerians. The Latin word "N.B." conveys a sense of officialness and is often used in official memos, government advisories, etc. The phrase "LET THEM ALL BENEFIT" utilises words that benefit everyone, making people feel that it is for the benefit of the community, not just them.

At the grammatical level, the message begins with a simple sentence in the present perfect tense: "NDDC began ₦50,000 Monthly Stipend Payments." Although it uses the simple past tense, it sounds as though it has already begun. This gives a brief, factual foundation for the rest of the instructions. The reader will think that independent verification will show it is still in progress. Next, it uses passive voice in: "All Nigerians youths are advised to submit their account number for payment." This removes any responsibility from an individual and sounds like official government or civic service language. The use of the passive voice also helps in manipulative ways, such as not revealing who gave the advice, making it seem official through

the familiar sentence structure and making it seem like a group decision rather than someone telling you to do it.

This phishing message has employed a number of figures of speech and other rhetorical devices to enhance its persuasive power, build trust in the institution, elicit emotions and go viral through social sharing. The phrase "NDDC began ₦50,000 Monthly Stipend Payments" is a claim made in the form of fact, which is a form of what is called the rhetoric of actuality, the idea that something has already begun. It ascribes agency to NDDC in order to make the group sound legitimate, a group that is capable of beginning payments, implementing a program and awarding stipends. It uses exaggeration in the phrase "All Nigerian youths" in order to attract a large audience and elicit a sense of belonging. It is using the amount "₦50,000" as a figure that is irresistible in order to overcome scepticism because it is a generous amount. The direct address is achieved through words and phrases such as "check if your name is shortlisted" and "submit your account number." It has a personal touch and increases the reader's interest by addressing them as if they may already be on the list of beneficiaries.

Datum 7



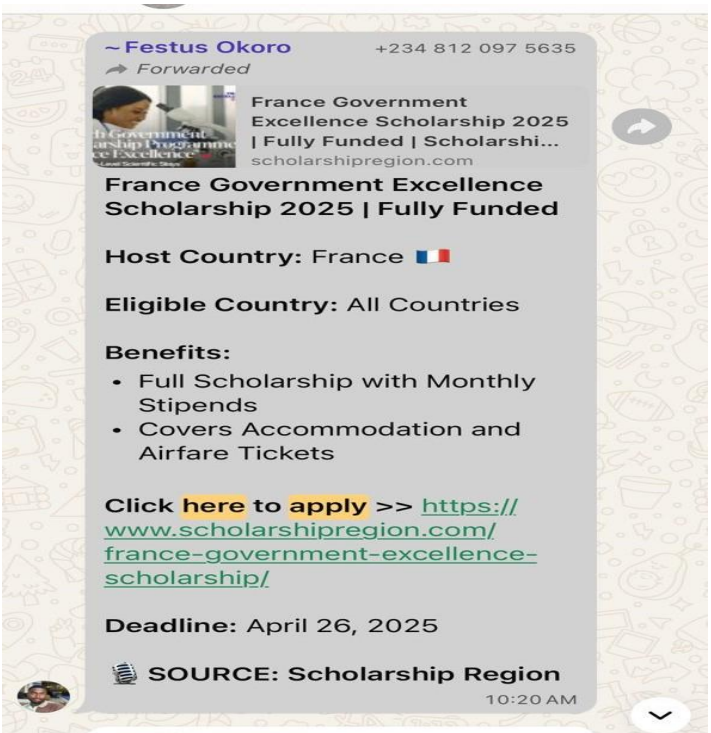
In terms of lexis, there is an evident intention to use certain words related to celebrity culture, weddings, telecommunications bonus programs, and social media. These words are meant to create associations with excitement, fame, the celebrity couple, and desire, while at the same time complying with the common definition of celebrity promotions. "Peller and Jarvis" – the names mentioned in the message – are well-known to young Nigerians who watch live streams and social media celebrities, and their very mention creates a sufficient prompt for those interested in this particular couple. The "20GB Free Data" and "₦10,000 Airtime" make up two attractive rewards for the telecommunication service. The phrase "in Celebration of Their Wedding" makes the give-away believable by alluding to the concept of a wedding, an occasion of great cultural significance in Nigeria. The telecommunication networks "MTN," "Airtel," "Glo," and "9-Mobile" are the leading telecommunication networks in Nigeria, with the use of "For" before each giving the impression that there are easy choices for the followers. The domain name "tinydash.pro" has no connection with the couple as well as none of the four telecommunication networks, while the path "/Jp2026" is made up of two initials with the year, making the content current and campaign-specific.

The grammar structure of the phishing message, which is written in the name of Peller and Jarvis for the wedding give-away, reveals that the message has headings, phrases, and an organised list of choices. The message has been written to resemble a legitimate celebrity-

sponsored give-away. The message starts with a bold heading “Peller and Jarvis’ 2026 Wedding Celebration Offer.” It is a noun phrase with a governing possessive but not a sentence and informs about the presence of an offer without any verb that can be tested. It is then followed by a longer line: “Peller and Jarvis in Collaboration with MTN, Airtel, Glo and 9-Mobile to Provide 20GB Free Data and ₦10,000 Airtime to everyone in Celebration of Their Wedding.” It is still not a sentence but includes several other ideas joined together in an easily readable way. The infinitive “to Provide” shows intentionality and not a commitment that was actually promised. Nearly all the content words are capitalised to resemble a headline of a press release or company announcement.

The phishing message employs many figures of speech and talking points related to celebrity weddings. It is a persuasive message that relies on parasocial relationships, cultural significance and follower association, all while maintaining the celebratory tone that is common in Nigerian celebrity weddings. Metonymy operates through the four brand names, since “MTN,” “Airtel,” “Glo” and “9-Mobile” stand in the text not only for four companies but for their consent, their resources and their corporate goodwill, none of which has been given. The inclusion of the names “Peller and Jarvis” is a form of parasocial intimacy that relies on the one-sided relationship between a follower and a celebrity, and for a follower who has watched their content daily, the names evoke positive emotions such as affection, success and celebration, which is why the phishing message is appealing through language. Hyperbole is present in the promise of a benefit “to everyone” and in the size of the reward, since a giveaway of that scale to an unlimited number of recipients would represent an expenditure that no private couple could sustain. The repetition of the pattern “For MTN,” “For Airtel,” “For Glo” and “For 9-Mobile” is a form of anaphora that produces an orderly and generous rhythm.

Datum 8



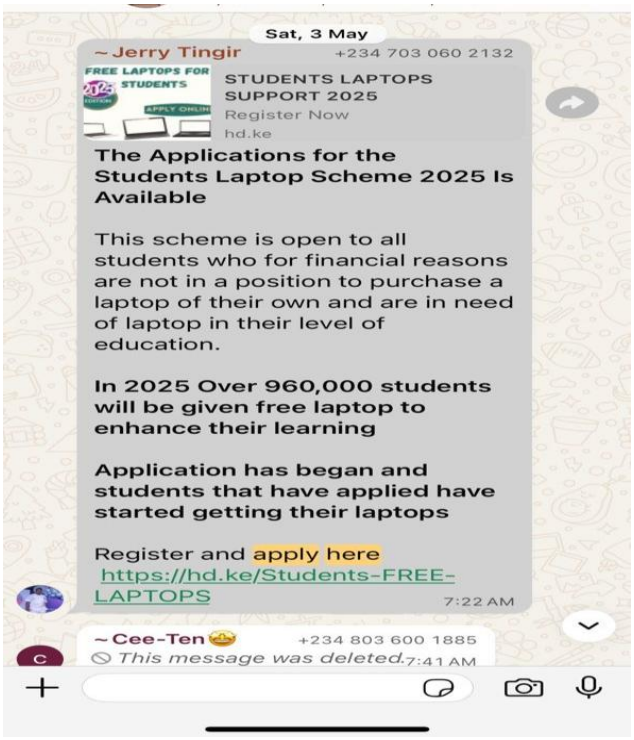
Words used make the recipient feel hopeful, trusting, and in need of time, which makes it appear legitimate. Words like "France Government Excellence Scholarship," "Fully Funded," "Host

Country: France," and "Eligible Country: All Countries" make the reader feel legitimised and unique, capitalizing on the prestige of the French government when it comes to educational opportunities and government scholarships. The word "Fully Funded" is especially valuable because it implies that the scholarship will pay for everything needed, overcoming the main obstacle to studying abroad. The use of words like "France," "Host Country," and "All Countries" provides a wide international scope of the opportunity and ties it to a popular European country. The words used are positive and grand, such as "Excellence," "Scholarship," "Monthly Stipends," "Accommodation," and "Airfare Tickets," appealing to people's dreams and aspirations related to education and career. This is supported by the fact that feelings can impact a person, as educational opportunities can be very motivational, or in other words, the "pathos" can play an important role in people's lives. It is important to note that using the word "Stipends" in the phishing message is smart, as "stipends" are actual monetary aid to pay living expenses, and that seems to be more attractive to students from developing countries than "help" with expenses. The wording "Monthly Stipends" suggests continuity and sounds appealing. Specifying the exact dates such as "2025" and "April 26, 2025" provides the reader with some degree of accuracy; this is one of the phishing techniques aimed at minimizing the level of skepticism of the reader. The word "Scholarship Region" suggests some credibility since the information is provided from the educational website. The word "SOURCE" in the capital letters refers to credible sources.

It should be stated that the structure of the phishing message is quite simple, but it is uncommon. It makes abundant use of noun phrases and direct statements but no orders or commands whatsoever. Unlike many other phishing messages, it is consistent with the theme of the message. In this case, the message has been written using many nouns as well as incomplete sentences missing a subject. In fact, it uses short sentences that act as information headers rather than full sentences like "France Government Excellence Scholarship 2025 | Fully Funded," "Host Country: France FR," and "Eligible Country: All Countries." This is similar to the way a notification for any scholarship is written where the primary concern is the concise communication of information rather than the formation of complete sentences. These header information parts do not have finite verbs and therefore give an objective presentation of information that need not be justified. This reduces the likelihood of questioning in an effort to seek justification. In the section describing benefits, the short noun phrase format has been used: "- Full Scholarship with Monthly Stipends," "- Covers Accommodation and Airfare Tickets." Here, in the latter case, the verb "covers" has been used whereas in the former it hasn't.

The phishing message contains many rhetorical devices and techniques typical for the genre of the education opportunity. The effectiveness of this message is increased by means of references to international prestige, benefits, clear deadlines, and a factual tone characteristic of scholarly notices. The text "France Government Excellence Scholarship" is a good example of a rhetorical device combination, where each single word or phrase helps to form the persuasive impact. "France Government" refers to national prestige and prestige of education in France; "Excellence" refers to people's self-image and values of merit; and "Scholarship" refers to education opportunities and advancements. These three words form a combination of prestige, which is then used to persuade via a set of related ideas. The message contains the repetition of words "Fully Funded" to highlight the message and attract attention of the recipient.

Datum 9



Graphologically, the message makes strong use of bold text in the heading "**FREE LAPTOPS FOR STUDENTS**" and the subsequent line "**STUDENTS LAPTOPS SUPPORT 2025**", which gives it a sense of officialness and opportunism, much like real students' programmes or government support programs. It also stands out through its strong use of typography and emotionally charged words. It also has a clear structure, with the command "Register Now" prominently displayed beneath the bold heading, a short-looking domain "hd.ke" that still gives the impression of a real website and a horizontal line used to separate the header from the body of the message, mimicking the look of real formal announcements. The text appears to be written in basic paragraph form. The text includes the phrase "The Applications for the Students Laptop Scheme 2025 are available" to indicate that the offer is currently valid. The text also includes a figure that is considered significant, "Over 960,000 students will be given free laptops to enhance their learning." The figure is significant because of the large number, even though it is not bolded. There is a link included, "https://hd.ke/Students-FREE-LAPTOPS" The domain “hd.ke” represents a Kenyan top-level domain that may appear geographically appropriate. The link includes the word "FREE-LAPTOPS" to make the offer sound more appealing. The text includes a timestamp, "7:22 AM," indicating the message was sent at that time. The timestamp is included to make the message look more authentic, as if it were actually sent by a person. The message includes basic spacing, a clear order and a professional look, similar to a school message. The message is an example of how phishing messages can look legitimate, which can be difficult for students who are seeking this kind of help to notice.

At lexical level, the use of words like education, money concerns and technology are used to create the idea of wanting more, trust and urgency. The message uses common ideas about student help schemes. The message uses words like "STUDENTS," "LAPTOPS," "Scheme," "Applications," "learning," "education," etc., which are commonly used in the field of education to convey a sense of legitimacy by leveraging society's values of education. The word

"FREE LAPTOPS" is very appealing to students because it addresses a common financial barrier to purchasing technology. The text includes emotional and need-based words like "financial reasons," "not in a position to purchase," "in need of laptop," and "enhance their learning." These words evoke emotional connections to subjects such as education, money and the need to do well in school. They seem to follow the pathos appeal, as education is very important to the students and their parents. The phrase "financial reasons" conveys the idea that there is not enough money and the audience will be able to identify with the statement. The use of numbers like "2025," "Over 960,000 students," and "7:22 AM" seems to convey the impression that the statements are factual and the use of numbers is a popular technique to remove all doubt. The word "Over 960,000 students will be given free laptops" is a big exact number used to show the scope of the matter. It shows a large, well-funded programme that is already working and covers a lot of people. "The students that have applied have started getting their laptops" shows the programme is already working, providing benefits. It is a form of social proof. "Register Now" creates a sense of urgency. "Apply" on the link is the same idea.

A grammatical check of the message reveals a pattern of clear statements, present tense urgency and the use of passive and active voice. This creates the illusion of a legitimate, established programme by making the scam more believable through the way it is written. The message begins with strong, clear statements of fact in the present tense: "**FREE LAPTOPS FOR STUDENTS**" and "**STUDENTS LAPTOPS SUPPORT 2025.**" These are noun groups, making them read as fact rather than opinion or belief, requiring evidence or belief in their truthfulness. The next sentence, "Register Now," is written in the imperative voice, making it a smooth transition from statement of fact to request for action. The text begins with the statement "The Applications for the Students Laptop Scheme 2025 are available," indicating the present tense to highlight the chance. The grammatical error "Applications... Is" is not very noticeable, but it has the effect of actual spoken language. The passive voice "will be given free laptop" in "Over 960,000 students will be given free laptop" makes the students seem to be receiving assistance from some external agency and the actual agency providing the assistance is not made clear. The present perfect "have started getting their laptops" in "students that have applied have started getting their laptops" indicates the finished action and the effect, giving the impression that the action has been started and the effect continues. The use of "to enhance their learning" indicates the purpose and the benefits and it relates the acquisition of a laptop to education. The command "Register and apply here" is an example of combining two commands, a concise way to keep the text brief. The text is composed of simple sentences throughout, avoiding complex ideas and making it useful for reading on phones. The tense changes on purpose. It uses the simple present tense ("is," "are"), the simple future tense ("will be given") and the present perfect tense ("have started"). This establishes a time frame that indicates an immediate opportunity and a history of actions. It appears to be an established institution with a history of success, which instils trust.

This phishing message incorporates many figures of speech and rhetorical devices, which make it more persuasive to students. The phrase "FREE LAPTOPS FOR STUDENTS" is a combination of persuasive words. It includes the word "FREE," which resolves the money problem. It includes the word "LAPTOPS," which represents the need for technology. Finally, it includes the word "FOR STUDENTS," which represents the people who will benefit from the offer. This word helps the message feel more relevant and acceptable because it represents a sense of belonging. Therefore, the phrase represents a desirable solution that will have the greatest impact because it includes what students want and need. The words "STUDENTS" and

"LAPTOPS" are repeated in the headings and the text. This is a rhetorical device used to make the idea more prominent. The words "for financial reasons are not in a position to purchase a laptop of their own" demonstrate an understanding of their financial issues. This evokes sympathy because it indicates to the recipient that the speaker understands their circumstances and, therefore, they will be less resistant. The words "in need of a laptop in their level of education" portray a laptop as something a student needs to learn. This reinforces the argument that this is a good thing and will make the recipient feel less guilty for accepting it.

Datum 10



At the lexical level, the words are intended to instil trust, foster ambition and create a sense of urgency while also relating to general ideas about employment within the public sector. The phishing message employs official-sounding words like "FEDERAL CIVIL SERVICE COMMISSION," "FCSC," "Recruitment," "Application Portal," and "Apply." The words are meant to evoke a sense of government authority and official hiring procedures while drawing on the positive image of Nigeria's federal civil service to lend authenticity. The full name is repeated twice: "FEDERAL CIVIL SERVICE COMMISSION RECRUITMENT 2025." The use of "Application Portal Now Open" indicates the use of the present tense to convey that this is an opportunity available right now. The word "Portal" refers to the online application system used by the government to recruit, which gives the application process a tech-savvy look.

The grammatical analysis of the message reveals a grammatical construction comprising statements, questions, commands, passive and active voice. The grammatical construction ensures the phishing message appears to be a legitimate, ongoing recruitment process, thereby compelling the reader to take action through the authority it conveys. First, the grammar construction of the phishing message is "FEDERAL CIVIL SERVICE COMMISSION RECRUITMENT 2025." Further on, "FCSC Application Portal Now Open" is written in the phishing message. The grammatical construction is formed with a very simple noun phrase where the recruitment process is treated as a fact, thus avoiding any ambiguity. The variation of

grammatical constructions in using both "FEDERAL CIVIL SERVICE COMMISSION" and "FCSC" does not affect the name of the organisation at all. The unique question asked in the message is: "Are You Skilled, Courageous and principled? Nigeria Needs You." This is the only question in the message. It has several functions: It speaks to the reader in the second person, asks the reader to respond affirmatively and then launches into the next sentence. The list of adjectives, "Skilled, Courageous and principled," repeats the same structure and so sounds more balanced and easier to remember. The second sentence, "Nigeria Needs You," is in the simple present tense and has Nigeria as the subject. The directive "Apply And Also Share To Others, there might Be Someone Who Needs This Opportunity" uses a series of commands like "Apply" and "Share," and also provides a reason with "there might be someone who needs this opportunity." This makes the directive slightly softer while still providing a command.

In terms of rhetoric, the phishing message tries to convince the reader by using elements of patriotism, individual eligibility and the general good, while being formal like a job ad of the government. Each word contributes to the sense of legitimacy: "FEDERAL" conveys a sense of nationhood, "CIVIL SERVICE" implies stable government jobs, "COMMISSION" implies a formal body of individuals, "RECRUITMENT" implies jobs are being filled and "2025" implies timeliness. The cumulative effect of these words is meant to create a sense of authority to persuade the reader. The question "Are You Skilled, Courageous and principled?" employs a well-known tactic of engaging the reader by relating them to these positive attributes. The use of a three-word list (tricolon) makes the message more memorable and persuasive. This list moves from being good at something to being courageous and then being principled. This enhances the moral sentiment and strokes the egos of those who share the same opinions. The subsequent phrase, “Nigeria Needs You,” is an example of an apostrophe because it refers to the country as if it needs something. This will make people feel nationalist sentiments and be concerned about contributing to their country and not just in getting a job. This is because the phrase incorporates both the personal qualities and the contribution to one’s country.

Discussion of Findings

The analysis of phishing messages in this study revealed systematic patterns of linguistic manipulation across six scam types, addressing each of the four research questions through a comprehensive stylistic and rhetorical examination.

Analysis of lexical elements in all the phishing messages shows that fraudsters make use of carefully selected lexical items from certain semantic fields that create a feeling of trustworthiness, urgency, and desire. Government scams (Federal Civil Service Commission, NELFUND, Child Support Fund) consistently make use of lexical items such as “Federal Government,” “President Bola Ahmed Tinubu,” “Minister,” “registration portal” and “entitled” that create contexts of institutionalisation through exploiting credibility of existing institutions and politicians. Corporate scams (MTN, OPay) make use of names of organisations together with lexicon related to the telecommunications industry (“SIM CARD,” “GB,” “data,” “airtime”) and vocabulary associated with marketing (“anniversary,” “bonus,” “gift,” “reward”). The religiously-oriented scams (WF-AID Ramadan, OPay Ramadan) include sacred greetings (“Salam alaikum,” “Ramadan Kareem”) and culturally significant terms (“dates,” “essential items,” “muslims in need”). Messages that include celebrities (Davido's wedding) take advantage of popular culture portmanteaux ("CHIVIDO") and celebrity names to trigger parasocial relationships. In all message types, number-specificity (specific amounts such as ₦50,000, 10GB, 100GB) gives rise to an illusion of transparency, whereas emotionally-charged words such as "free," "hurry," "congratulations," "deserving," and "eligible" evoke an emotional

response. The use of imperative language ("Click Here," "Apply Now," "Register," "Submit Account") limits the autonomy of the reader, and thus compels him/her to respond immediately.

A grammatical analysis shows that the phisher uses syntactic arrangements that use the style of declarative statements, imperative commands, strategic tenses, and intentional departure from Standard English. The declarative mood is common for all the phishing messages, with phrases like "The National Youth Empowerment Fund Application Form 2025 Is Out" and "Every Nigerian is entitled to receive" making fraudulent declarations appear as statements of facts that require no proof. The present tense and present progressive ("is offering," "registration is ongoing," "Portal Now Open") give the assurance of the current validity and immediacy of action. Imperative mood is prevalent in calls for action ("Hurry Now," "Click Here," "Apply," "Share," "Submit Account"), which lack any polite forms and establish the tone of authority that precludes deliberation on behalf of the recipients.

In the analyses, use of all the types of rhetoric is found to be present. The figure of speech, personification is very common in all forms of phishing. For example, in "The National Youth Empowerment Fund vision is to give out" the abstract organisations have been provided with human intentionality and benevolence for the development of the cause. Use of hyperboles like "150,000 – 550,000 grant," "100GB for 10 years plus," "Over 960,000 students will be given free laptops" makes it certain that hyperboles have been extensively used in order to overwhelm the recipient's sense of skepticism through generous offers. Metaphors like "helping hand" have been used to depict financial help as charity. Direct address in form of apostrophe has been used by addressing the recipients.

Research Findings

From the above general discourse in relation to the four research questions, the following conclusions can be drawn from the stylistic analysis of phishing messages:

1. Scammers employ carefully selected lexical items: institutional and government terms in the FCSC and NDDC data (Datums 3, 5, 6 and 10), corporate and brand terms in the MTN and OPay data (Datums 1 and 4), and religious and celebratory terms in the Dantata and wedding-giveaway data (Datums 2 and 7), combined throughout with numerical specifics and emotionally loaded words to gain authority and overcome scepticism.
2. Phishing messages combine declarative and imperative statements, strategic tense choices and, in some of the data (Datums 3, 5, 6 and 9), passive constructions, alongside occasional grammatical deviations, in order to imply authority, urgency and authenticity while saving the reader's cognitive processing time.
3. Figures of speech, such as personification and hyperbole in the youth-empowerment and laptop data (Datums 5 and 9), metonymy and anaphora in the celebrity-wedding data (Datum 7), and code-switching in the Dantata data (Datum 2), work together to increase emotional involvement and lower critical distance.
4. Across the data, fraudsters combine appeals to ethos by invoking known institutions and public figures (Datums 3, 5, 6 and 10), pathos through urgency and emotionally loaded language (Datums 2, 5, 6, 8 and 9), and logos through the appearance of official procedure and numerical precision, mirroring the classical rhetorical structure adapted from Hoyland (2001).

Conclusion

The stylistic examination of phishing messages from various scam genres, including mimicking government, brand hijacking, religion scam, celebrity worship, educational scam, and poverty alleviation scam, shows that scammers on the internet are skilled, flexible, and ethically corrupt stylists who use linguistic convention, symbolism, institutional credibility, and human

vulnerability to reach their fraudulent ends. It is shown that phishing messages are not primitive and easily identifiable but complex deceptive messages that use a highly developed combination of graphology, lexicon, grammar, discourse, and rhetoric to deceive a particular target audience. The combination of Leech and Short's stylistic approach with rhetorical theory (Aristotle, as cited in Hoyland 2001) offers an effective analytical tool for understanding how these linguistic choices work together to manipulate readers and help scammers achieve their fraudulent goals.

Based on these findings, telecom regulators and platform operators are recommended to develop automated flagging systems that watch for the recurring stylistic signatures identified here, such as urgency imperatives paired with government or brand names and improbably generous numerical offers, rather than relying solely on spelling errors or blacklisted links. Cybersecurity awareness campaigns should teach the public to recognise these specific rhetorical strategies — ethos built on borrowed institutional or celebrity credibility, pathos built on urgency and communal obligation, and logos built on precise but unverifiable figures — since recognising the strategy is more transferable than recognising any single scam. Digital literacy programmes, particularly those aimed at students, job seekers and first-time WhatsApp users, should incorporate examples drawn from real Nigerian scam messages of the kind analysed here so that recognition skills are grounded in the local context in which these scams actually circulate.

References

Adu-Manu, K. S., Ahiable, R. K., Appati, J. K., & Mensah, E. E. (2022). Phishing attacks in social engineering: A review. Journal of Cyber Security and Information Systems, 4(4), 239–267. https://www.techscience.com/JCS/v4n4/53755

Ahmad, R., Terzis, S., & Renaud, K. (2024). Getting users to click: A content analysis of phishers' tactics and techniques in mobile instant messaging phishing. Information & Computer Security, 32(4), 420–435. https://doi.org/10.1108/ICS-11-2023-0206

Ajayi, T. M. (2022). Discursive-Manipulative Strategies in Scam Emails and SMS: The Nigerian Perspective. Lodz Papers in Pragmatics, 18(1), 175–195. https://doi.org/10.1515/lpp-2022-0008

Ariyanto, Z. R., & Rahmawati, L. E. (2024). The form and meaning of language motifs in phishing crimes: A forensic linguistic study. LITE: Jurnal Bahasa, Sastra, dan Budaya. https://doi.org/10.33633/lite.v21i1.11463

Arsyad, A., Hakim, A., & Astria, I. (2021). Aristotle's rhetorical theory and its relevance in modern communication. International Journal of Multicultural and Multireligious Understanding, 8(4), 190–198. https://doi.org/10.18415/ijmmu.v8i4.2541

Ashiru, A. (2021). Identifying Phishing as a Form of Cybercrime in Nigeria. Nnamdi Azikiwe University Journal of International Law and Jurisprudence, 12(1), 1-15.

Aziz, A. A. A., Azhar, S. B. H. J., Yatim, A. I. A., Hamid, A. A. A., Nordin, N. A., Zabidin, N. S., & Asmawi, A. (2021). Modelling the language of cyber scammers: A forensic linguistics analysis of Malaysian illegal investment scheme. International Journal of Academic Research in Business and Social Sciences, 11(6), 1612–1621.

Carter, E. (2023). Confirm not command: Examining fraudsters' use of language to compel victim compliance in their own exploitation. The British Journal of Criminology, 63, 1405–1422. https://doi.org/10.1093/bjc/azac098

Charles, L. (2023). Uncovering cybercrime tactics: Studying emerging linguistic features and forms of Swahili fraudulent SMS in Tanzania. Journal of Emerging Technologies. https://doi.org/10.57040/z07jkm33

Chiluwa, I. M., Chiluwa, I., & Ajiboye, E. (2018). Online deception: A discourse study of email business scams. In T. Docan-Morgan (Ed.), Deception & deceptive communication: Motivations, recognition techniques and behavioural control (pp. 169–188). Nova Science Publishers.

Daily Independent. (2026, May 7). Nigeria is the most spammed country in Africa. Daily Independent, 20(2156).

Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2021). Human Factors in Phishing Attacks: A Systematic Literature Review. ACM Computing Surveys, 8(4), 88-102. https://doi.org/10.1145/1122445.1122456

Halliday, M. A. K., & Matthiessen, C. M. I. M. (2014). Halliday's introduction to functional grammar (4th ed.). Routledge.

Hashim, S., et al. (2017). Language and deception in phishing communication. [Full publication details to be confirmed by the author.]

Hassan, R. (2021). Style and stylistic choice in communication. [Full publication details to be confirmed by the author.]

Hoyland, C. (2001). Rhetoric in the Modern World: Applications of Aristotelian Principles.

Hua, T. K., Abdollahi-Guilani, M., & Zi, C. C. (2017). Linguistic deception of Chinese cyber fraudsters. 3L: The Southeast Asian Journal of English Language Studies, 23(4), 108–122.

Taylor, M. (2019). Digital literacy and cybersecurity awareness. [Full publication details to be confirmed by the author.]

Jolaiya, O. A. (2024). The effect of electronic fraud on the financial performance of deposit money banks in Nigeria. Asian Journal of Economics, Business and Accounting, 24(4), 10–20. https://journalajeba.com/index.php/AJEBA/article/view/678

Lazarus, S., & Okolorie, G. U. (2019). The bifurcation of the Nigerian cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) agents. Telematics and Informatics, 38, 1–10. https://doi.org/10.1016/j.tele.2019.01.002

Leech, G. N., & Short, M. (2007). Style in fiction: A linguistic introduction to English fictional prose (2nd ed.). Pearson Longman.

Nlebedum, C. J. (2017). Dear valued customer: A forensic-linguistic analysis of scam texts. An Unpublished Master's thesis, University of Lagos.

Olasehinde, T. (2024). The evolution of phishing attacks: Tactics and countermeasures. ResearchGate. https://www.researchgate.net/publication/385091892

Romanenko, A. (2017). "Rhetorical Devices in Advertising: Persuasion Through Language." Journal of Media and Communication Studies, 9(3), 45–53.

Taiwo, R. (2021). Discursive forms and functions of digital deceptive communication in Nigerian online discourse. Academia.edu. https://www.academia.edu/66218598/DISCURSIVE_FORMS_AND_FUNCTIONS_OF_DIGITAL_DECEPTIVE_COMMUNICATION_IN_NIGERIAN_ONLINE_DISCOURSE

Whitty, M. T. (2024). The victimology of online fraud: A focus on romance fraud victimisation. Journal of Economic Criminology, 3, 100053. https://doi.org/10.1016/j.jeconc.2024.100053

Xu, T., & Rajivan, P. (2023). Determining psycholinguistic features of deception in phishing messages. Information & Computer Security, 31(2), 199–220. https://doi.org/10.1108/ICS-11-2021-0185