Scammers' Identities as Represented in Emails to Indonesian Journal Editors

Deny Efita Nur Rakhmawati[1(✉)], Rohmani Nur Indah[1], Habiba al Umami[1], Muzakki Afifuddin[1], and Hujuala Rika Ayu[2]

[1] UIN Maulana Malik Ibrahim Malang, Malang, Indonesia
denyefita.nr@bsi.uin-malang.ac.id
[2] State University of New York, New York, USA

Abstract. Numerous scam emails received by journal editors with various rhetorical techniques are considerable linguistic phenomena to examine. Certain rhetorical techniques provide information about the email senders' identity and ideology. Thus, this study employs the transitivity system of Halliday's Systemic Functional Linguistic and Chiluwa's discourse strategies to discover how scammers construe reality based on their identities and ideologies. The findings show that the highest number of data provide powerful relational discourses, whether the discourse is explicitly stated or implicitly inferred through the narrativity of the emails. Based on those findings, the represented identity of the scammers is understood to be ambiguous: whether the scammers have power or have learned to express power in their writing. The ambiguity, however, is proven ironic by the findings on the misapplication of Standard English writing, which also provides evidence that the scammers are most unlikely highly educated. Even though this study does not provide evidence of the real identity of the scammers, this study has provided confidence for the recipients to easily acknowledge that the scammers are the ones who have less power than the recipients do.

Keywords: Scam emails · Identity · Systemic Functional Linguistic

1 Introduction

The current fact shows the rapid network on the internet in the circulation of fraud via email. It belongs to one of the effects of easy access to information in the global era and the enactment of the free market. More studies are currently exploring the characteristics of emails that are detected as fraudulent. One of the results shows that linguistically, fraud via email uses a lot of modal verbs intending to direct, promise, threaten, and even show the function of politeness. The use of modal verbs significantly contributed to the success of these scam emails [1]. Furthermore, the email sender tries to take a personal approach; therefore, the linguistic feature shows the choice of pronoun, namely first person singular [2]. In terms of lexicogrammar, the choice of the scammer clause is dominated by orientation to familiarity, directly mentioning the destination, and explicitly requesting a transfer [3].

R. N. Indah et al. (Eds.): AICOLLIM 2022, ASSEHR 725, pp. 5–15, 2023.
https://doi.org/10.2991/978-2-38476-002-2_2

The widespread use of scam emails with various rhetorical techniques is one of the significant linguistic phenomena to examine. Even though the email is sent massively without knowing each of the target recipients, the sender can change the name and address to cover their real identity. They can show the impression in a highly personalized manner [4]. Viewed from the content of the email, the rhetorical move is constructed in such a way to make it more convincing to the recipient. If the receivers do not carefully understand the rhetorical pattern of the email, they will fall into the trap of scammers. Through concise sentence construction, the rhetoric used can touch the receiver's egocentrism [5]. Few scam emails begin with narrative content to attract readers' sympathy. Here, they try to be creative by playing with artistic words so that the receivers sympathize and follow up on the request in the emails [6].

The scam emails have certain features that are easier to recognize from the discourse structure. At first, the scammers tried to get along and steal sympathy so that the email recipients began to trust them as the parties who help, invite cooperation, impress with kindness, and can be promising partners [7]. That is why caution is needed in identifying emails that lead to fraud under the guise of an offer of cooperation [8]. However, the more people understand the characteristics of scam emails in terms of discourse and linguistics, the less the risk of becoming a victim of fraud. Thus, it is clear that cybercrimes need to be removed immediately, and no more fraudulent emails take their toll [9].

Initially, research into email scams stemmed from the massive scams in Nigeria. Nigerian emails are easy to spot as fraudulent emails from the past. From the linguistic features of its content, the fraudulent messages contain elements of realism shown in their persuasive lexical choices [10]. Some dictions often appear as "urgent" and "secret". Besides, the sentence structure often leads to grammatical, mechanical, and vocabulary errors, indicating that the email's sender is not in native English [11]. However, it is clear that the orientation of the expression is to win the sympathy and trust of the email recipient [12]. The discursive model of Nigerian email has a distinctive ideological and identity pattern. The sender tries to construct an identity that can make the victim sure to make a decision quickly without having any bias or prejudice that there is an element of fraud [13].

In general, fraudulent emails are quite popular, and even digital natives make it a joke these days. From the analysis of psychological persuasion, fraudulent emails have certain characteristics of settings, scenarios, framing, and signals [14]. The typology of fraudulent emails apparently invites the creativity of netizens through online communities that massively seek to uncover the identities of scammers and discuss them on their social media. If at first, scammer emails were often ignored, but now netizens have the potential to develop them for the entertainment aspect [15].

Technological advances also have a role in the dynamics of email scammers. Due to the large number of spam emails that are very annoying and wasting time, nowadays, more and more content-based machine learning techniques are being developed to filter emails, separating spam emails [16]. On the other hand, fraudulent email senders also made a number of innovations by referring to effective experiential, interpersonal, and textual aspects. Based on their experience, victims are more easily caught with a more appropriate choice of language [17]. Furthermore, even today's email content can be translated automatically so that it can reach a wider coverage of recipients.

This study derives from the assumption that the identity of the sender is closely related to the content of the scam email, either explicitly or implicitly, in constructing the ideology represented. It is because scammers try to form an identity that makes email recipients feel familiar and personally involved [6]. The identity of the sender of the scam email is also implied from the narrative construct that is presented as evidence to increase the recipient's trust [13]. Even scammers these days are also increasingly skilled in displaying their identity as ordinary people who use language politeness strategies to the maximum to lure victims [17].

Therefore, for reliable linguistic proof, this study employs the transitivity system of Halliday's Systemic Functional Linguistic to discover how scammer construe reality based on their identities and ideologies. The transitivity system is a system that reveals the ideational metafunction reflected in the text believing that every participant, process and circumstance involved in the text are intentionally chosen by the author of the text for the sake of maintaining particular ideologies, thoughts, and beliefs [18] which result in sustaining particular identities in social discourse.

Furthermore, this study also utilizes Chiluwa's discourse strategies to portray the scammers' identity through the way they construct the discourse structures of their emails. The structures consist of discourse initiation or self-identification, narrativity or tellability, reassurance and confidence building, confidentiality offering, and action prompting tact [19]. The variation strategies utilized by the scammers are the space in which scammers' identities are performed and justified [20].

With the development of linguistic discourse related to email scammers, empirical findings are still needed on how scammers show ideological representation in the content of their emails. So far, the existing research has only reviewed scammer emails sent to personal recipients [1–3]. As for institutional receiver addresses, it is still questionable whether there are differences in the typology of email content scammers. In this study, the scam emails observed were those sent to the email address of the journal editors at a university in Indonesia.

2 Method

This study employs a qualitative approach since it aims to descriptively uncover the phenomenon within the text and discourse. The data are scam emails sent to the journal editors' email address which is written in the list of editorial teams in the online journal system. The data sources are classified based on the scammers' roles in the text. Only utterances that position the scammers as the participant of the sentence become the data. The data are then analyzed using Halliday's transitivity system and Chiluwa's discourse strategies. Finally, the result of the transitivity system and discourse strategies are discussed by revealing the way the author of the text construes reality drawn through ideology and identity represented within the text.

3 Findings and Discussion

3.1 Findings

3.1.1 Transitivity System

There are five types of processes found in the scam email. Material processes are found in the highest number, while existential processes are found in the lowest number. The result is listed in Table 1.

From 26 material processes found, seven verbs are linked to the highly mentioned circumstance, money or wealth. Such processes are expressed through the verbs that indicate a transfer of possession. They are *give, donate, offer, invest, compensated, recover,* and *nominated*. These verbs embed in the email sender as the actor of the process and the addressee of the email as the recipient. The use of material processes denotes the highest power strata in the context. It is because the action of the material processes has particular impacts on the goal-participant or the recipient [18]. In this case, money, as the circumstances of the process, denotes a social strata-changer tool of human beings, making someone richer changes the social status of the society. Therefore, in the case of scam emails toward the journal editors, the scammers position themselves as powerful participants in the discourse, which enables them to change the state of being of the journal editors by giving out a huge amount of money.

Meanwhile in the behavioural process, the most found verb is *decide.* Other verbs found are *need, urge, ensure, bless,* and *wait*. As a halfway process of material and mental processes, the behavioural process indicates a condition of the behaver which stands between the physiological and psychological. The verb as *decide* shared the characteristic of material and mental processes. Such verb denotes an action that is not materially done but has a particular impact on the other participants. In the case of the scam email, though the senders have positioned themselves as the most powerful participant, they hand out the decision of accepting the offer (money) to the email recipient. It reflects that the senders respect the boundaries of other participants in the discourse. It makes the scammers polite person because with the power they have, they do not force the other participants.

However, though the most verb found in the behavioural processes reflects boundaries between the scammers and the recipients, some mental processes expressed through *God*

Table 1. Types of Processes

Type of Process	Number
Material	26 (37%)
Behavioural	15 (21%)
Mental	16 (23%)
Relational	12 (18%)
Existential	1 (1%)
Total	70 (100%)

bless and *peace be with you* denote a struggle to break down the boundaries. As the closure of the emails, it functions to assure the recipients that the scammers are good people like them. Therefore, the recipients may leave out their worries and put some trust in the scammers. Not to mention, the most found verb used to express mental process is *appreciate.* It portrays the scammers' positive attitude toward the email recipients. The process reflected through this verb enhances the powerful position of the scammers than the other participants involved in the discourse. It is because only the powerful one can appreciate while the powerless one can only feel grateful, though *appreciate* and *grateful* express the same mental state of being. Thus, the powerful state of the scammers is expressed materially, through the material process, and mentally, through the choice of verbs in expressing the mental process.

The two least processes found in scam emails are relational and existential processes. Relational processes found in the scam email are used as a greeting by introducing the writer of the scam email, though it does not guarantee that the name mentioned is the scammers' real names. In scam emails, the relational processes portrayed as an introduction imply that the scammers are strangers to the emails' recipients. In detail, the scammers embed their prestigious position in their workspace to the relational process in the text. It portrays their accountability as the emails' senders.

In addition, the existential process is only found within the expression *Below is my Phone/WhatsApp number! I* ***am available*** *via WhatsApp as an alternative to email should this be a preference.* While most scammers prefer to get in touch with the recipient through email, least to none scammers take the communication phase to a more personal communication gadget. It augments the relationship distance between the participants. The scammers implicitly denote that they do not want to shorten the relationship distance between them and the recipients. A notion of stranger reflected through the relational processes is enhanced by the preference of communication contact reflected in existential process.

Based on the transitivity system reflected in the processes above, the identity of the scammers embedded within the scam email is a powerful polite stranger. In addition, the ideology reflected is "money as the symbol of power but its power cannot be a justification to disrespect other people's boundaries". The scammers are powerful because they have money yet are polite enough to leave the decision to accept the money to the recipients.

3.1.2 Discourse Structures

There are five discourse strategies applied by scammers in their emails. The highest strategies employed by the scammers are the narrativity or tellability and the action prompting tact while the lowest one is occupied by the reassurance and confidence building strategy. The results could be seen in Table 2.

All the scam emails sent to the journal editors adopt the narrativity or tellability strategy. The narratives of the scam emails are mostly outspoken and in business patterns. The business designed emails are in the similar construction, consisting of introduction, body, and conclusion [9]. Among the scam emails sent to the journal editors, the introduction are in the general polite greetings, such as *"dear beneficiary", "my dear friend", "dear friend", "hello friend",* and *"good day dear friend".* Then, these introductions lead off the body narrative which usually about the tellability or story of death, terminal

Table 2. Discourse Strategies

Type of Process	Number
Narrativity or tellability	11 (27%)
Discourse initiation/self-identification	7 (17%)
Confidentiality offering	3 (7%)
Reassurance and confidence building	9 (22%)
Action prompting tact	11 (27%)
Total	41 (100%)

ill person who share the inherited fortune, or the profit that needed to be claimed, like *"I have in mind to invest … the fund i inherited from my late husband but my present health can't permit me to handle this divine project by myself", "Before His Death my father Deposited $4.500.000.00 in Escrow unit",* and *"I discovered that my branch in which I am the Manager made excess profit of [US$12.5 Million dollars] which my head office is not aware of and will never be aware of"*. Then, the narratives ended with a considerate and formal closing, such as *"sincerely", "yours respectfully", and "respectfully"*. This narrativity places the scammers as organized and advanced professional persons who acknowledge the procedures of dealing with and compromising respectable business who attempt to engage with the scammed as the discourse participants.

Besides, the scammers also deceive the email recipients with the amount of money, fund, investments, such as *"you are one of the lucky 40 winners that the committee has resolved to compensate with the sum of (€2,000,000.00 Euro)", "I am contacting you to stand in as a next of kin to his deposit of ($ 9Million USD)For investments purposes", "I have nominated you as my beneficiary to receive 1000 kg of Gold Dust/Gold Dore Bar, which is estimated today at more than (Fifty Seven Million Euros) (€) 57,000,000. + plus $10,000,000 (USD) cash."* By referencing certain numbers of money, the scammers convince to enrich the scammed. It indicates that the scammers manipulate the scammed by presenting themselves as generous and wealthy figures who strive to help others.

Though the scammers place themselves as a decent businessman or wealthy humanists, they cannot hinder their inabilities in producing standard varieties of English. It could be seen from their misspelling in an email address, such as "*The Scott foundation*", but the email domain name says *"@scotfoundation.org*" and "*Shirin Hamid from the Economic Community of West African State Institution*" which is not listed as a domain in the email address "ms.ruthdesmond8@gmail.com", inconsistent or no punctuation, like in "(IMF) International Monetary Fund. in alliance with economic community of West African states (ECOWAS)We have been working towards the eradication of fraudsters and scam Artists in the world", and the use of capital letters, such as "*Before His Death my father Deposited $4.500.000.00 in Escrow unit"*. These struggles portray that the scammers are from non – English speaking countries and failed to fulfill the narrativity. They abort to present their identities as real professional and respectable persons.

In addition, from 7 discourse initiation or self-identification, 5 of them start their emails with introducing themselves. They mention their names and professions including

the titles, such as in *"This is John R. Oxford, Jr. of the U.S. Army Aviation and Missile Research, Development, and Engineering Center (AMRDEC) based in Africa's Sahel region."* This self-identification is started by mentioning the scammers' names and professions, as they are unknown persons to the email recipients. By indicating their names, the scammers attempt to undertake online introductions and build intimacy with the email recipients. Furthermore, the scammers' professions are acknowledged as they want to manifest their existences as professionals who acquire certain advanced skills in certain fields.

Moreover, the scam email is also initiated by the use of flowery words, as the scammers intend to catch the attention of the emails receiver and engage with them conveniently. This kind of initiation is accomplished to restrain any pattern of doubtful in the received email [9]. "*I know it is quite unacceptable and unethical breaking into your privacy in this manner, but this calls for urgency as I would want to divulge this information to you"* is one the initiations of the scam email which attempt to engage the receivers by manipulating them with a nature of politeness and pretending to show the urgency of sending the email. The intention also reflects that the scammers demand the faith of the recipients on the delivered messages in the email. Thus, they expect that the recipients will trust and execute any idea the scammers addressed in the email. Moreover, it indicates that the scammers strive to maintain their identities as the credible figures.

Furthermore, 9 of 11 scam emails denote that the scammers assure the scammed to build trust and put any worries away. The scammers assure the scammed by mentioning *"I believe it could be the key to achieving lifetime success without the necessity of taking any risks" "I am not a greedy person",* and *"You are to make sure that you received the UN Approved DISCOVER CARD in your names"*. In this case, the scammers frequently assure the scammed that their shared information in the emails is legitimate and harmless. In order to do this, they employ tactics for boosting certainty and confidence. They reassure the receivers with statements or promises which is done in straightforward manipulative tactics. It denotes that the scammers are the trusted and legitimate persons. They have the power to control the situation and guarantee the validity of their emails.

Ironically, some scam emails highlight the importance of maintaining secrecy and emphasize the recipient's genuineness, honesty, and confidence. The confidentiality could be found in *"I hope you will not double cross a uniform brother in active service who has sacrificed in keeping America and the world safe."* It indicates that the scammers urge the recipients to be sincere, trustworthy, and confident. In these situations, the scammers hardly suggest the scammed to put the emails confidential and not being thoughtless by sharing them with the publics, but it may also be done with the intention of giving the recipient a false sense of security so that they will unwittingly invest in the "business" without telling anyone else about it. These techniques also suggest that scammers are good manipulators in convincing the recipients to finalize the deal without going through formal legal processes or talks. Falsely implying that confidentiality and trust are necessary for the transaction; however, the scammers just commit fraud.

Interestingly, all scammers sign off their scam emails with the action prompting tact. They demand the recipients' response and act fast. *"As soon as I receive your response through this Address (wa222747@gmail.com)", "Your quick response will*

be highly appreciated", "Your prompt response and support would be most gratefully appreciated", and *"I wait for your quick response to help me send you the details"* are some of the suggestions of the scammers to the scammed to give immediate responses. Here, the scammers position themselves as the important persons who have the power to demand the scammers to give prompt reactions. Simply said, the scammers also put themselves as legitimate figures who deliver underlined and bolded essential messages to seem genuine and convincing.

As highlighted above, according to the discourse strategies employed by the scammers in the scam emails sent to the journal editors, the identity of the scammers is a generous legitimate foreigner. Additionally, the ideology reversed in the scam emails is money is a manifestation of the credibility and trustworthiness behind the falsification. Therefore, the scammers are credible and use money to support their stands.

3.2 Discussion

In findings, it appears that scammers apply expressions that denote a mental state of reality to gain sympathy and reflect a positive attitude. One of the examples is praying or expressing hope for the recipient of the email with the expression: "May God bless you as you extend your helping hand to a uniform member of the U.S armed forces" (datum JO), "Peace be with you" (datum EE), "God bless" (datum AA). The scammers attempt to attract sympathy through such prayer sentences as part of the strategy to build closeness with the recipient of the email. This is in line with the finding of Taiwo's research that scammers engineered their sentences based on a number of experiences they had related to how sentence constructs were proven to be effective in winning the hearts of email recipients [17]. Additionally, with prayer as the closing sentence of the email, the scammer seeks to establish an identity as a kind and wise person to lure potential victims.

Scammers sending emails to Indonesian journal editors were very aware of the role of settings and scenarios in constructing the conveyed identity. The settings mentioned in the findings always involve countries far from Indonesia, namely the United States (Datum ER, JO), West Africa (datum SH), Libya (datum JV), Syria (datum AA), and Ghana (datum MW). In some emails, the settings were not stated explicitly, only explaining scenarios such as investment cooperation (datum BM, SG, CM), and humanitarian missions (datum EE, MS). These findings are in accordance with the results of Neuhaus' research that setting and scenario will form a scammer's communication pattern in addition to the selection of framing methods and signals toward fraud [14]. In this case, it is clear that recognizing the email settings and scenarios is an important step in examining the scammer's email typology.

From the construction characteristics of the emails sent to Indonesian journal editors, it can be concluded that there are a number of violations in terms of narrativity and precision. For example, in datum AA, the narrative mentions "The Scott foundation", but the email domain name says "@scotfoundation.org", which indicates a spelling error. In another email there is a difference in the identity of the name in the email narration of "Shirin Hamid from the Economic Community of West African State Institution" which is not listed as a domain in the email address "ms.ruthdesmond8@gmail.com" (datum SH). Another error appears in the narrative email as "Mariana Davies Dominick, a US

military officer" but sent from the email address "daviphilomene@gmail.com" (datum AA). Mislabelling of names in the narration also appears. The full name of "Michael Williams Anderson" in the narration is shortened to "Michael Williams" in the sender's identity. The scammer should have mentioned the first and last name, not the first and middle name. It is what Taiwo suspects as a violation in discursive construction [13]. Therefore, it can be concluded that the emails sent to the Indonesian journal editors did not pay attention to the aspects of narrative discourse and precision, thus making it easier for the editors who received the email to suspect an element of fraud.

Scammers always try to amaze email recipients by providing adequate explanations when introducing themselves as the identity of important and respectable people. Among them are philanthropists who want to donate in large amounts (datum MS, EE), important officials who give prizes to lottery winners (datum SH, ER), humanitarian volunteers who offer collaboration (datum AA, JO), executives of large companies who offered profit sharing (datum JV, MW), and beneficiary inviting business cooperation (datum CM, BM). It is what Carter mentioned as a way for scammers to maintain their identity through a strategy of inferring legitimacy and credibility [4]. What they maintain is legitimacy and credibility, such as showing rank, affiliation, and contact to particular email address.

In addition to issues related to narrative discourse, mentioning nominal of money and capital dominates the emails sent to Indonesian journal editors. As acknowledged by Onyebadi and Park, the contents of email scammers cannot be separated from terms related to tangible human needs, such as money, the need for economic improvement, business benefits, profitable investments, and the like [10]. In the finding, it was stated that the amount of money used to lure victims varied, namely $6,850,000.00 USD (MS datum), $1.8million US Dollars (SH datum), US$68,760,000.00 (JV datum), €2,000,000.00 Euro (ER datum), 40% of US $12.5 Million dollars (MW datum), $4,500,000.00 (CM datum), $9Million USD (BM datum), and 40% of $10M USD (JO datum). The terms used to describe money are also variously mentioned. The findings of this study are also similar to those found by Chiluwa et al., that mention the terms such as money transfer, investment, inheritance claim, next-of-kin claim, charity donation, foreign aid, and foreign account lottery [9].

4 Conclusion

The fact that the identity represented within the scam emails is ambiguous and ironic is unexpected by this study. The ways the scammers utilise their knowledge on providing power in position and funds and on providing sympathetic stories are proven to be the opposite. Even though the real identity of the scammers is still unknown, this study has provided strong evidence that the possibility that real identity of the scammers are far different from what they have provided. This study hopefully provide insights for not only other researchers but also authorities to further study scam emails especially on the believability of the narrative in the perspective of other readers.

References

1. Chiluwa, I. M., & Anurudu, S, Expressing (Un) certainty through Modal Verbs in Advance Fee Fraud Emails, in: Covenant Journal of Language Studies 8 (1), 2020.
2. Alli, R., Nicolaides, R., & Craig, R., Detecting advance fee fraud emails using self-referential pronouns: A preliminary analysis, in: Accounting Forum 42 (1), 2018, pp. 78–85.
3. Anafo, C., & Ngula, R. S., On the grammar of scam: transitivity, manipulation and deception in scam emails, in: Word, 66(1), 2020, pp. 16–39.
4. Carter, E., The anatomy of written scam communications: An empirical analysis, in: Crime, Media, Culture 11(2), 2015, pp. 89–103.
5. Freiermuth, M. R., Text, lies and electronic bait: An analysis of email fraud and the decisions of the unsuspecting, in: Discourse & Communication *5*(2), 2011a, pp. 123–145.
6. Hiß, F., Fraud and fairy tales: Storytelling and linguistic indexicals in scam e-mails, in: International Journal of Literary Linguistics 4(1), 2015.
7. Freiermuth, M., "This transaction is 100% risk-free!" Why do people fall prey to e-mail scams?, in: International Conference on Language and Communication (LANCOMM), 2011b, pp. 222–230.
8. Chiluwa, I., "Congratulations, Your Email Account Has Won You€ 1,000,000": Analyzing the Discourse Structures of Scam Emails, in: The Palgrave handbook of deceptive communication, Palgrave Macmillan, Cham, 2019, pp. 897–912.
9. Chiluwa, I. E., Ovia, E., & Uba, E., "Attention Beneficiary…!": Assessing Types and Features of Scam Emails, in: Handbook of Research on Deception, Fake News, and Misinformation Online, IGI Global, 2019, pp. 421–438.
10. Onyebadi, U., & Park, J., 'I'm Sister Maria. Please help me': A lexical study of 4-1-9 international advance fee fraud email communications in: International Communication Gazette, 74(2), 2012, pp. 181–199.
11. Schaffer, D., The language of scam spams: linguistic features of "Nigerian fraud" e-mails, in: ETC: A Review of General Semantics, 2012, pp. 157–179.
12. Rich, T., You can trust me: A multimethod analysis of the Nigerian email scam, in: Security Journal, 31(1), 2018, pp. 208–225.
13. Taiwo, R., Orevaoghene, A., & Adebukunola, F., Social media and discursive construction of rumours in Nigeria, in: Ife studies in English Language, 13(1), 2017, pp. 69–94.
14. Neuhaus, T., A Nudge Psychology Perspective on Digital Marketing and Communication: Learning from the Nigerian Scam, in: Innovative Perspectives on Corporate Communication in the Global World. IGI Global, 2021, pp. 122–140.
15. Dynel, M., & Ross, A. S., You Don't Fool Me: On Scams, Scambaiting, Deception, and Epistemological Ambiguity at R/scambait on Reddit in: Social Media+ Society, 7(3), 2021.
16. Mohan, M., Detection and Prediction of Spam Emails Using Machine Learning Models, in: Handbook of Research on Cyber Crime and Information Privacy. IGI Global, 2021, pp. 201–218.
17. Taiwo, R., Discursive manipulation strategies in virtual scams in global contexts, in: Computer-Mediated Communication across Cultures: International Interactions in Online Environments, IGI Global, 2012, pp. 143–154.
18. Halliday, M.A.K. & Matthiessen, C., An Introduction to Functional Grammar, London: Arnold, 2004.
19. Chiluwa, I., The discourse of digital deceptions and "419" emails, in: Discourse Studies, 11(6), 2009, pp. 635–660. https://doi.org/10.1177/1461445609347229.
20. Bamberg, Michael., Narrative Discourse and Identities, in: Narratology beyond Literary Criticism, 2005, https://doi.org/10.1515/9783110201840.213