Semantic Urgency and Illusion of Authority in Phishing Emails: A Corpus-Based Analysis

Rossy Halimatun Rosyidah

Universitas Pamulang, South Tangerang, Banten, Indonesia
dosen02145@unpam.ac.id
*corresponding author

ARTICLE INFO

Article history
Received June 10 2025
Revised July 25 2025
Accepted August 22 2025

Keywords
Keyword_1 Phishing Discourse
Keyword_2 Semantics Frame
Keyword_3 Fillmore
Keyword_4 Corpus

ABSTRACT

This study examines how urgency and authority are semantically framed in phishing emails to manipulate recipients' behavior. Although linguistic features of deception have been widely studied, the semantic framing of phishing remains underexplored within the Frame Semantics framework. Using qualitative frame-semantic discourse analysis, ten phishing emails were purposively selected from the open-access corpus by Miltchev et al. (2024), focusing on scams related to account access and payment issues. The data were analyzed through Fillmore's Frame Semantics to identify lexical units and frame elements (e.g., Agent, Goal, Instrument) that trigger urgency and authority. Results show that phishing messages use time-sensitive cues (e.g., immediately, within 24 hours) and institutional references (e.g., your account, verify your identity) to create a sense of crisis and compel compliance. These frames often co-occur, increasing cognitive pressure and reducing critical evaluation. By mapping manipulative strategies onto semantic frames such as Request, Threat scenario, and Commerce transfer, this study provides a structured approach to phishing analysis. It contributes to cyber linguistics and supports the development of frame-aware digital literacy, email security systems, and spam detection models based on semantic cues.

This is an open access article under the CC–BY-SA license.

1. INTRODUCTION

Phishing is one of the most prevalent forms of cyber threats, relying heavily on linguistic strategies to manipulate victims into actions that compromise personal data and security. Phishing emails commonly employ language that conveys urgency and authority to elicit emotional and cognitive responses such as fear and trust (Baryshevtsev & McGlynn, 2020; Tian, Jensen, & Bott, 2024). Scammers often exploit the perceived authority of institutional actors, such as banks or IT departments, to create a sense of legitimacy and pressure recipients to comply (Forte, 2009; Wright et al., 2016). Messages containing direct threats or appeals to authority reduce critical evaluation and increase recipient compliance (Wright et al., 2016; Baryshevtsev, M., & McGlynn, 2020).

Although phishing has been extensively studied regarding its frequency and impact, much existing research has focused on technological countermeasures or superficial linguistic features. Studies examining phishing discourse from a deep semantic-pragmatic perspective remain limited. Most works emphasize user behaviour or the tone of messages, but fail to uncover how underlying semantic mechanisms function to create persuasive

effects. This gap highlights the opportunity to analyze phishing through the theoretical framework of Frame Semantics, which provides a structured approach to understanding how urgency and authority are conceptually framed in phishing language.

Some previous studies have analyzed various linguistic aspects of phishing texts, such as conciseness, wording, and impoliteness (Shafqat et al., 2016; Guo et al., 2023). Other research has addressed the psychological effects of appeals to urgency and authority in relation to user compliance (Altmann et al., 2017; Baryshevtsev, M., & McGlynn, 2020). However, these studies have primarily focused on observable or behavioral features without delving into the underlying semantic patterns. For instance, while Shafqat et al. (2016) identified tone-based deception and Guo et al. (2023) examined politeness, none systematically analyzed how linguistic units activate conceptual structures of meaning through a frame-semantic approach. These works have concentrated mainly on surface-level features or behavioral outcomes, neglecting to thoroughly examine the semantic construction of urgency and authority in phishing discourse. The conceptual mechanisms by which phishing messages evoke specific emotional and cognitive frames among recipients remain underexplored.

Although other studies have recognized the relevance of urgency and authority, few have critically applied semantic analysis to examine their construction within phishing messages. The theoretical contribution of this study is unique because it applies frame semantics in the context of phishing discourse, an approach that has not been systematically used to date. Similar to other research investigating surface linguistic details or psychological influences of phishing messages, this study builds upon them by identifying the conceptual frames phishing messages employ regarding the receiver. The semantic-pragmatic approach offers a new perspective through which the linguistic construction of urgency and authority in phishing can be examined.

This study hypothesizes that phishing messages combine urgency and authority frames through specific lexical and syntactic patterns to elicit recipients' emotional responses and diminish their critical resistance. These frames are semantically embedded in directive forms and institutional references that systematically co-occur within phishing discourse. This hypothesis is grounded in the theoretical premise that phishing messages strategically employ urgency and authority to influence recipients' cognitive and emotional processes. The study contributes to cyber linguistics and offers practical insights for enhancing digital literacy and developing effective phishing protection measures based on interpreting these semantic structures. Specifically, this research addresses the following questions: How are the meanings of urgency and authority semantically constructed in phishing messages? Which linguistic patterns systematically activate these frames to produce manipulative effects in phishing discourse?

To examine these questions, this approach employs the semantic frame theory advanced by Fillmore (1982), which considers meaning to be created by conceptual frames, conceptually structured background knowledge activated by specific linguistic items. The relevance of Frame Semantics in phishing analysis lies in its ability to model how specific lexical units, such as *verify*, *suspend*, or *update*, evoke abstract structures of meaning familiar to users, such as requests, sanctions, and institutional authority. Potential threats caused by urgency frames in phishing emails create a sense of necessity due to time

pressure, while authority frames involve references to institutions or social rules, generating a sense of obligation and authoritarianism (Narayanan et al., 2002; Baker, 2017). Interactions between these frames produce powerful manipulative messages, which reduce the cognitive resistance of the recipients and make them more compliant (Chrysanthou et al., 2024; Orman, 2012).

Analysis of the semantic composition of these frames holds value for the theory of cyber linguistics and digital literacy practice. The finding that phishing messages strategically employ linguistic tools to target recipients can contribute to developing improved phishing literacy campaigns and anti-phishing tools. Building on this theoretical foundation, further examination of how these frames operate in discourse sheds light on their manipulative power and practical implications. The structure of urgency and authority frames in phishing discourse exemplifies how language exploits conceptual expectations associated with specific linguistic cues to influence recipients. This interaction intensifies persuasive pressure and diminishes critical resistance. A close analysis of the internal semantic construction of these frames underscores the study's relevance to theoretical discussions in cyber linguistics and practical initiatives in digital literacy. Identifying the mechanisms through which particular lexical items trigger coercive frames may inform the design of more effective phishing education programs and terminology-sensitive anti-phishing defence systems.

These frames trigger cognitive and emotional schemas in the reader's mind, influencing how they interpret and respond to phishing messages. For example, a message such as "Your account will be locked in 24 hours" activates the urgency frame, exposing the user to a time-sensitive threat, whereas "Please verify your identity with your bank" invokes the authority frame, appealing to institutional authority. Understanding how these frames operate and interact provides insight into the linguistic processes phishing attacks use to manipulate recipients. Therefore, by applying a semantic-pragmatic framework, the linguistic patterns and frame elements present in phishing messages can be systematically analyzed, generating insights into the subtle tactics of digital deception. These insights contribute both to theoretical understanding and practical advancements in cybersecurity (Narayanan et al., 2002; Baker, 2017).

To examine the semantic structure of urgency and authority in phishing messages, this study employs Fillmore's (1982) frame semantics theory, focusing specifically on how urgency and authority cues serve as framing features that trigger manipulative strategies. Frame Semantics, as applied here, facilitates the identification of the conceptual scaffolding underlying linguistic manipulation in phishing, where lexical units activate conceptual frames structured knowledge patterns that systematically influence interpretation.

Regarding urgency cues, these are lexical or syntactic stimuli that evoke frames related to time pressure, impending danger, or opportunity. For example, when a sender uses phrases such as "immediately" or "within 24 hours," the receiver is constrained by a time frame, often leading to hasty and sometimes unwise decisions. This phenomenon, known as the bare urgency effect, implies that individuals are more likely to prioritize less critical tasks when marked as urgent, as the sense of urgency carries intrinsic value that can alter decision-making priorities (Zhu et al, 2018). At the neurological level, urgency cues

influence the activity of brain areas responsible for risk assessment and emotion recognition, such as the striatum and insula, thereby affecting behavioral motivation under time pressure (Jones et al., 2011).

Furthermore, authority cues instigate legitimacy, social power, or role frames within an organization, usually by invoking relied-upon or official recognition, or through imperative vocabulary. Examples of duty-related phrases include "authenticated by your bank," "official wording," or modal words like "must," which produce a sense of duty and demand action through the power of speech, compelling others to act in ways they might not have without the psychological manipulation of "power language" (Joullié et al., 2021). Typically, subjects are coerced by appeals to their perceptions of legitimate power and social expectations (Tyler & Jackson, 2014).

These cues collectively compose manipulative strategies and language techniques that reduce cognitive resistance and heighten recipients' responsiveness. The synergy between urgency and authority frames creates a dual manipulation structure, increasing the likelihood of user compliance. Their co-occurrence provides persuasive coherence that often overrides user scepticism. This synergy exerts convincing pressure on readers to take immediate and uncritical action, which is central to the deceptive power of phishing. By identifying and examining these cues through Frame Semantics, this study aims to uncover the underlying semantic processes phishing messages employ to influence users.

2. RESEARCH METHODOLOGY

This study adopts a qualitative interpretive approach through frame-semantic discourse analysis to examine how urgency and authority are semantically constructed within phishing texts. The interpretive approach emphasizes understanding phenomena within their specific contexts, allowing researchers to capture the nuances of meaning in complex communicative situations (Nurdin, N., & Pettalongi, 2022). Additionally, interpretive studies typically involve collecting rich, qualitative data to gain detailed insights, which supports in-depth analysis of textual constructions such as those found in phishing messages (Décosse et al., 2013). To operationalize this interpretive approach, the analysis is grounded in Frame Semantics theory (Fillmore, 1982) and supported by the FrameNet conceptual framework (Baker, 2017). This approach enables an investigation into how specific word combinations in phishing sentences trigger the activation of conceptual frames that influence readers' interpretations and cognitive processes.

This study adopts an interpretative and analytical approach. As Elbardan & Kholeif (2017) note, it goes beyond merely describing word usage by delving into the semantic structures triggered by specific lexical choices, combining interpretive insights with systematic qualitative analysis. The analysis centers on two dominant frames, urgency and authority, which are believed to work in tandem to exert persuasive pressure on recipients. Following the principles of qualitative interpretation, this exploratory inquiry aims to examine how meaning is constructed in phishing messages closely.

Data were obtained from the Phishing Validation Emails Dataset (Miltchev et al., 2024), an open-access and peer-reviewed corpus on the Zenodo platform. This corpus is widely cited in cyber-linguistic research and contains 2,000 email samples, comprising 100 labelled phishing emails, 730 safe emails, and 1,170 unlabeled emails. The corpus

metadata includes columns such as "Email Type," "Sender," and "Subject," which enable precise filtering of phishing content.

These studies only considered the clearly labelled phishing emails, as indicated in the "Email Type" column of the Phishing Validation Emails Dataset (Miltchev et al., 2024). Ten phishing sentences were purposively selected from this subset to enable detailed semantic analysis. The sample was chosen based on open inclusion criteria: (1) the sentence had to contain imperative verbs and lexical indicators of urgency or authority; (2) syntactically, it had to be complete, with a determinable subject and predicate; and (3) it had to serve phishing purposes such as stealing credentials, account suspension, or requests for verification. Sentences that were fragmentary, contextually ambiguous, or deliberately incomplete were excluded. The selection of ten samples reflects the concept of analytical saturation in qualitative semantic studies (Varekamp, 2014), striking a balance between dense and representative analysis without sacrificing interpretive depth.

Therefore, the analysis was conducted manually using the Frame Semantics approach, guided by an interpretative coding model to reveal how phishing messages embed manipulative discourse through lexical framing. The procedure involved five analytical steps. First, each phishing sentence was segmented into lexical tokens to isolate meaningful units relevant to manipulation (e.g., *verify*, *click*, *within 24 hours*). This tokenization provided a granular view of the language choices that potentially activate conceptual frames.

Next, trigger words, lexical units suspected of evoking frame-level meanings, were identified. Words such as *update*, *confirm*, *claim*, and *verify* were considered likely to activate semantic frames related to institutional or transactional contexts. Each lexical unit was then matched with corresponding frame entries in FrameNet. Frames such as *Authentication*, *Threat scenario*, *Commerce transfer*, *Sanction*, and *Reward acquisition* were selected based on their conceptual alignment with the context and pragmatic function of the sentence.

Once the appropriate frames were activated, their associated Frame Elements (FEs) were manually annotated. These included core roles such as Agent, Goal, Credential, Authority Source, Deadline, and Manner. The annotation was based on contextual cues and the syntactic realization within each phishing sentence. Finally, the relationship between authority and urgency was analyzed by classifying manipulative strategies. Each sentence was coded, and the outcomes of the co-occurrence of time-sensitive cues and institutional voice were examined in terms of their effect on increasing psychological pressure, cognitive overload, and persuasive compliance.

To visualize this process, the following figure summarizes the research flow:

Corpus Selection » Sentence Tokenization » Lexical Trigger Identification » Frame & Frame Element Annotation » Manipulation Strategy Classification & Triangulation

Figure 1. The five-stage analytical framework is from corpus selection to strategy classification and triangulation

Therefore, to illustrate the annotation process, Table 1 below presents representative examples from the analyzed corpus. The table shows examples of how lexical units in phishing sentences trigger semantic frames and frame elements, contributing to manipulative strategies.

Table 1. Manual annotation of urgency and authority frames in phishing sentences

Phishing Sentence	Lexical Unit	Frame	Frame Elements	Manipulative Framing
"Update your payment information immediately"	Update	Commerce transfer	Agent: User; Goal: Payment Info; Time: Now	Urgency + Institutional Authority
"Your account has been suspended by the bank"	Suspended	Sanction	Target: Account; Authority: Bank	Authority via Threat
"Click here to verify your account now".	Verify	Authentication	Agent: User; Credential: Account; Manner: Now	Urgency + Authentication Frame

The annotation process in this study was conducted manually, using definitions from FrameNet as the primary reference. No computational tools were employed, such as FrameNet parsers or NVivo software. However, the coding adhered to consistent semantic criteria to ensure accuracy. Although an intercoder agreement was not reached, two validation strategies were implemented to enhance the reliability of the analysis.

First, data triangulation was applied by comparing the selected phishing sentences with legitimate (non-phishing) emails from the same corpus. This comparison helped confirm that manipulative cues, such as expressions of urgency and authoritative voice, were specific to phishing. Second, theoretical triangulation was employed by incorporating insights from Speech Act Theory (Searle, 1979) and Cognitive Load Theory (Sweller, 2011). These theories supported the interpretation of how linguistic framing generates psychological pressure and encourages compliance.

Despite careful procedures, this study has several limitations. The sample size was small, consisting of only ten phishing sentences, limiting the findings' generalizability. The entire analysis was conducted by a single researcher, potentially introducing bias in frame identification and meaning interpretation. Additionally, no behavioral testing was performed, leaving the real impact of these messages on users unknown. Furthermore, the dataset included only English-language emails, so the findings may not be applicable across different languages or cultural contexts.

The limitations provide helpful directions for future research. Consistency could be improved by involving multiple coders and assessing intercoder reliability (e.g., through calculating Cohen's Kappa). Experimental methods, such as eye-tracking or response time testing, could be conducted to understand better how recipients process these messages. Expanding the dataset to include multiple languages and geographical regions would

enhance the generalizability of the findings. Finally, increasing the efficiency and scalability of the analysis may involve using semi-automated tools for frame detection.

3. FINDINGS

The findings of this study show that phishing messages deliberately employ the language of urgency and authority by framing them systematically. As stated in the research objective, the study explores how certain words or phrases, called lexical triggers, activate specific semantic frames that contribute to manipulative strategies in phishing communication. Using Frame Semantics as a foundation, the analysis demonstrates how sentences in phishing emails activate frames such as *Sanction*, *Commerce transfer*, and *Authentication*, collectively creating pressure on the reader. This section also highlights how urgency and authority frequently co-occur and reinforce each other in phishing discourse. These frames are not used randomly; instead, they are carefully woven into the surface structure of language to influence recipients' emotions and cognition. Through Frame Semantics, the study reveals how specific words trigger conceptual meanings (frames) and how their grammatical forms strengthen the message's manipulative intent.

Ten representative phishing sentences were purposively selected from a validated open-access corpus to explore this in detail. Each sentence was analyzed by identifying the lexical triggers, the activated frames, the relevant Frame Elements (FEs) according to FrameNet, and the manipulative strategies involved. Particular attention was given to how the Urgency Frame and Authority Frame interact and combine into broader semantic manipulation, which functions to lower the recipient's critical resistance and increase compliance. This entire process followed the five-stage analytical framework described in the methodology, from sentence tokenization to the classification of manipulative strategies.

Table 2. Frame-semantic analysis of phishing sentences

No.	Phishing Sentence	Lexical Unit	Frame	Frame Elements	Manipulative Framing
1	Your account has been temporarily suspended... Please verify...	suspended	Sanction	Offender: account; Authority: bank; Sanction: suspension	Deontic threat + impersonated authority
2	Important notice: Your payment was declined... Update your payment...	update	Commerce transfer	Agent: user; Goal: payment info; Time: immediate	Institutional command + urgency pressure
3	Alert: Unusual login detected... Confirm your identity now	confirm	Authentication	Credential: identity; Manner: now	Breach fear + verification imperative

4	Dear Customer, your subscription will expire... Renew immediately	renew	Service continuity	Client: user; Service: subscription; Time: 24h	Loss aversion + polite authority
5	Your payment failed due to security... Update within 12 hours	update	Transaction update	Agent: user; Object: info; Deadline: 12h	Sanction framing + deadline
6	Congratulations! You've won a prize... Claim your reward immediately	claim	Reward acquisition	Recipient: user; Goal: reward; Manner: immediately	Joy trigger + legitimacy framing
7	You have a secure message from your bank... Click here to read	message	Communication	Source: bank; Content: secure info	Institutional trust + command
8	Important: Update your email settings... avoid interruption	update	Technical change	Object: settings; Agent: user	Implicit threat + technical voice
9	Your payment was declined... Update billing to continue the service	update	Billing	Client: user; Object: billing info; Goal: service	Financial urgency + imperative tone
10	Your package is pending... Provide info to confirm delivery	confirm	Goods delivery	Goal: delivery; Info: personal details	Service legitimacy + identity surrender

Each phishing sentence in this study was analyzed through five steps: (1) breaking the sentence into parts (sentence tokenization), (2) identifying key words or phrases (lexical units), (3) determining which semantic frame is triggered, (4) identifying the elements within the frame (Frame Elements), and (5) classifying the manipulative strategy employed.

In Sample 1, the verb "suspended" activates the *Sanction* frame, where "your account" functions as the Offender, and the bank is positioned as the authority. The phrase "please verify your identity immediately" triggers the *Authentication* frame. The word "immediately" adds urgency by marking the *Manner* in which the action should be performed, combining both urgency and authority within a single sentence.

In Sample 2, the verb "update" triggers the *Commerce transfer* frame, where the user is the Agent and the payment information is the Goal. The word "immediate" again signals

urgency. Meanwhile, the phrase "Important notice" attempts to sound official, lending the message a sense of legitimacy and authority, despite being deceptive.

Sample 6 demonstrates a different technique. Here, the word "claim" activates the *Reward acquisition* frame. The message congratulates the reader, eliciting a positive emotional response. The word "immediately" is again used to create urgency. Unlike messages that use threats, one uses excitement and a sense of entitlement to persuade the reader, illustrating how emotions can be combined with time pressure to manipulate behaviour.

This detailed analysis shows that phishing emails frequently employ specific language patterns to pressure recipients. They use particular sentence structures, such as commands ("Click here," "Update your info"), polite expressions ("please"), and time-related words ("within 12 hours") to encourage swift action. These features reduce opportunities for critical thinking by making the message appear as a routine or professional request.

A key finding is that all ten phishing samples combined urgency and authority frames. None relied solely on one element. It suggests that the simultaneous use of both frames is more effective in persuading recipients, as it intensifies mental pressure and diminishes their capacity to question the message.

Furthermore, keywords such as "update," "verify," "confirm," and "claim" consistently corresponded to specific semantic frames in FrameNet, supporting the validity and robustness of the frame-based analysis.

In conclusion, phishing messages are persuasive not only because of their content but also due to carefully planned linguistic strategies. Frame Semantics helps reveal how these seemingly simple messages actually contain complex layers of manipulation. The combination of urgency and authority emerges as a key coercive method, which could inform improved phishing detection systems, educational programs for digital safety, and the development of linguistically informed cybersecurity tools.

4. DISCUSSION

This study aimed to understand how phishing messages create manipulative pressure by activating two key semantic frames: urgency and authority. By analyzing ten representative phishing sentences through frame-semantic discourse analysis, the research demonstrates that these frames are not used arbitrarily; rather, they are carefully embedded in both vocabulary and sentence structure to influence readers' thoughts and emotions. Phishing messages do not merely deceive; they are crafted using precise linguistic choices to manipulate the reader in subtle yet powerful ways.

One of the main findings is the consistent co-occurrence of both urgency and authority in all messages. Urgency never appeared independently; it was always paired with an indicator of authority, and vice versa. It suggests that successful phishing relies on the combined effect of both frames. The urgency frame is frequently triggered by time-related words such as "immediately," "within 24 hours," or "now." These terms shorten the perceived response time, thereby increasing psychological pressure.

From a psycholinguistic perspective, this aligns with Cognitive Load Theory (Sweller, 2011), which posits that time pressure increases mental load. Under such

pressure, individuals are more likely to respond hastily without fully processing information, making them more susceptible to manipulation.

Simultaneously, the Authority frame is constructed through language that mimics the style of official institutions. Phrases such as “your account,” “bank,” or “Dear Customer” evoke familiar social expectations of trust and responsibility. These expressions activate mental associations with credible institutions, lending legitimacy to the message. When combined with imperative sentence structures like “Update now” or “Click here,” the message adopts a tone of authority. This type of language carries what linguists term illocutionary force, meaning it functions as a genuine instruction or order. According to Speech Act Theory (Searle, 1994), such commands do more than convey information—they seek to prompt action from the reader. In phishing messages, this generates a sense of obligation or urgency, often by implying risk or duty. Thus, phishing messages imitate the speech style of authentic institutions to coerce users into compliance.

The contribution of Frame Semantics (Fillmore, 1982) is central to this analysis, serving not only as a theoretical framework but also as a practical tool. Each phishing sentence was decomposed into its core lexical units and mapped onto specific semantic frames from FrameNet, such as Sanction, Authentication, Reward Acquisition, Commerce Transfer, and Communication. These frames consist of specific constituents known as Frame Elements (FEs), including Agent, Goal, Credential, Deadline, and Authority, which appear across different phishing messages. For example, the verb “update” frequently triggers the Commerce transfer frame, in which the user is positioned as the Agent and the billing information as the Goal. This frame is typically accompanied by time-related expressions such as “within 12 hours,” which serve to construct a sense of urgency.

What makes phishing particularly manipulative is not merely the presence of individual frames, but the structured way in which they are combined. For example, in the sentence “Your account has been suspended. Please verify your identity immediately,” the Sanction frame is triggered by “suspended,” the Authentication frame by “verify,” and the Urgency frame by “immediately.” These overlapping frames create a layered message that cognitively overwhelms the recipient, increasing the likelihood of a swift response without critical evaluation.

Phishing messages often mimic familiar communication formats such as security alerts, payment notifications, or reward announcements. These recognizable genre frames activate common mental models of trusted organizational communication, such as technical support, service disruptions, or secure messaging. Lexical cues like “Important notice,” “secure message,” and “verify your account” are strategically used to make the message appear routine and credible, thereby masking the manipulative intent behind a tone that resembles legitimate institutional language.

Unlike other published studie, e.g., Alkhalil et al (2021); Guo et al. (2023); Baryshevtsev & McGlynn (2020), which predominantly focused on surface characteristics such as message tone, generic language expressions, or concealed URL addresses, this study offers a more nuanced examination. Applying a frame-semantic approach uncovers how phishing messages are structured through the consistent activation of conceptual frames and frame elements. This method goes beyond mere keyword identification by

revealing how meaning is systematically constructed to influence recipients' perception and behaviour.

Theoretically, this research contributes to the emerging field of cyber linguistics by demonstrating how Frame Semantics can be applied to model manipulative online discourse. As a diagnostic tool, frame-semantic analysis enables visualization of the "grammar of deception" embedded in phishing messages—illustrating how certain verbs, roles, and temporal markers interact to create high-pressure, high-legitimacy communicative acts. This contribution can inform the development of automated detection methods, where co-occurrence patterns between lexical triggers and Frame Element configurations are transformed into machine-interpretable rules for phishing classifiers.

Practically, these findings offer valuable insights for digital literacy education. For instance, educators can design simulated phishing messages based on common frame combinations, such as [Authentication + Urgency] or [Reward acquisition + Authority], to help users recognize and anticipate typical manipulation patterns. This approach trains individuals to become more alert to the ways language creates pressure or false authority. Furthermore, the findings have potential applications in the improvement of email-filtering systems. Rather than relying solely on blacklisted words or phrases, these systems could be enhanced by detecting manipulation through semantic patterns. Utilizing techniques like semantic parsing or natural language understanding, filters could identify phishing messages based on their frame combinations, thereby increasing detection accuracy and adaptability.

Despite these strengths, this study has several limitations. The sample size was relatively small, consisting of only ten phishing sentences, which restricts the scope and generalizability of the findings. Second, the coding and interpretation of frames were conducted by a single coder, lacking intercoder validation and thus risking interpretive bias. Third, the study focused exclusively on English-language data, overlooking potential cross-linguistic variations in phishing tactics. These constraints point to epistemological limitations inherent in qualitative, monolingual research.

Future studies should aim for triangulated, multilingual designs, incorporating larger corpora and cross-cultural comparisons, as well as experimental methods such as eye-tracking or reaction time measurements. Such approaches could investigate the cognitive effects of frame combinations and test whether the urgency-authority frame operates similarly across different languages and cultural contexts.

In conclusion, phishing discourse is not merely deceptive text but a form of structured semantic manipulation. The deliberate, synergistic activation of urgency and authority frames serves to heighten psychological pressure and create an impression of institutional credibility. By applying Frame Semantics to phishing communication, this research elucidates the mechanisms of digital manipulation and contributes to both theoretical and practical advancements in cyber linguistics and security-oriented discourse analysis.

5. CONCLUSION

The study further reveals that phishing messages are not only misleading in content but are also linguistically crafted to exploit cognitive responses by carefully activating both

urgency and authority frames. Drawing on Fillmore's Frame Semantics, the analysis demonstrates how lexical triggers such as "verify," "update," and "confirm" activate conceptual frames (e.g., Sanction, Authentication, Commerce transfer), each comprising a set of Frame Elements like Agent, Goal, Credential, and Deadline, which collectively steer the recipient toward compliance. This linguistic orchestration of frames uncovers not only surface-level manipulation but also a deeper semantic structure embedded within phishing discourse.

Building on this semantic framing, the study's principal theoretical contribution is the identification of the dual-frame construct—urgency and authority—as a structural characteristic of phishing discourse. This semantic pattern is not incidental but is programmatically embedded into phishing email phrasing through syntactic and lexical structures. The paper proposes that Frame Semantics can serve as a framework to model linguistic manipulation and includes a diagnostic schema adaptable to both human and automated phishing detection.

Practically, the findings have specific implications for the future design of NLP (Natural Language Processing) based spam filters, which could be enhanced by incorporating frame cues derived from targeted terms rather than relying solely on keywords. Moreover, this research provides a foundation for digital literacy training programs that equip users to recognize manipulative patterns through frame-based templates modelled on known phishing examples.

However, the study has limitations. The small sample of ten phishing examples limits generalizability and risks of overgeneralization. The analysis was conducted by a single coder without triangulation or intercoder reliability assessment, raising concerns about interpretive bias. Additionally, the study lacks empirical experimental data on how actual recipients respond to different framing interventions.

Future research should address these gaps by testing recipient susceptibility to urgency-authority framing in real time through experimental psycholinguistic methods, such as eye-tracking or event-related potentials (ERPs). Expanding the corpus to include multilingual phishing data would facilitate analysis of cross-cultural variations in frame usage. Further exploration of additional frame types, including Reciprocity, Threat scenario, and social proof, could deepen understanding of semantic manipulation across phishing genres.

In sum, this study contributes to the growing field of cyber linguistics by demonstrating that frame-based semantic analysis offers a replicable, theory-driven model for detecting phishing discourse. Recognizing the convergence of urgency and authority frames as a distinctive manipulation pattern may enhance both academic modelling and the practical effectiveness of countermeasures against digital deception.

REFERENCES

Alkhalil, Z., Hewage, C. T. E. R., Nawaf, L., & Khan, I. A. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers of Computer Science*, *3*, 563060. https://doi.org/10.3389/FCOMP.2021.563060

Altmann, E. M., Trafton, J. G., & Hambrick, D. Z. (2017). The effects of deadlines on task performance: Evidence for a cognitive resource limitation. *Journal of Experimental*

Psychology: General, 146(3), 457–472. https://doi.org/10.1037/xge0000268

Baker, C. F. (2017). FrameNet: Frame semantic annotation in practice. In *Advances in Frame Semantics: Theory and Practice* (pp. 771–811). Springer, Dordrecht. https://doi.org/10.1007/978-94-024-0881-2_28

Baryshevtsev, M., & McGlynn, T. (2020). Persuasive appeals predict credibility judgments of phishing messages. *Cyberpsychology, Behavior, and Social Networking*, *23*(5), 297–302. https://doi.org/10.1089/CYBER.2019.0592

Chrysanthou, Pantis, Y, Patsakis. (2024). The anatomy of deception: Measuring technical and human factors of a large-scale phishing campaign. *Computers & Security*, *140*, 103780. https://doi.org/10.1016/j.cose.2024.103780

Décosse, Molnar, Proper. (2013). A Qualitative Research Approach to Obtain Insight in Business Process Modelling Methods in Practice. In *The Practice of Enterprise Modelling* (pp. 161–175). Springer, Dordrecht. https://doi.org/10.1007/978-3-642-41641-5_12

Elbardan, H., & Rashwan Kholeif, A. O. (2017). *An Interpretive Approach for Data Collection and Analysis*. Cham: Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-54990-3_5

Fillmore, C. J. (1982). *Frame semantics. In Linguistics in the Morning Calm (pp. 111–137)*. Seoul: Hanshin Publishing Co.

Forte, D. (2009). Phishing Attacks: Phishing in depth. *Network Security Archive*, *5*, 19–20. https://doi.org/10.1016/S1353-4858(09)70055-8

Guo, Z., Wang, P., Cho, J.-H., Huang, L. (2023). Text mining-based social-psychological vulnerability analysis of potential victims to cybergrooming: Insights and lessons learned. *Companion Proceedings of the ACM Web Conference 2023*, 1381–1388. https://doi.org/10.1145/3543873.3587303

Jones, C. L., Somerville, L. H., Li, J., Ruberry, E. J., & Delgado, M. R. (2011). Under pressure: Response urgency modulates striatal and insula activity during decision-making under risk. *PLoS ONE*, *6*(6), Article e20942. https://doi.org/10.1371/JOURNAL.PONE.0020942

Joullié, J. E., Gould, A. M., Spillane, R., & Luc, S. (2021). The language of power and authority in leadership. *Leadership Quarterly*, *32*(4), 101491. https://doi.org/10.1016/j.leaqua.2020.101491

Miltchev, R, Rangelov, D, Genchev, E. (2024). *Phishing validation emails dataset (Version 1) [Data set]*. https://doi.org/10.5281/zenodo.13474746

Narayanan, S., Fillmore, C. J., Baker, C. F., Petruck, M. R. L. (2002). FrameNet meets the Semantic Web: A DAML+OIL frame representation. *Proceedings of the 18th National Conference on Artificial Intelligence (AAAI)*. https://aaai.org/papers/ws02-16-005-framenet-meets-the-semantic-web-a-damloil-representation-of-framenet/

Nurdin, N., & Pettalongi, S. S. I. (2022). An interpretive case study to understand online communication in an e-tendering project implementation. *Jurnal Manajemen Komunikasi*, *7*(1), 39. https://doi.org/10.24198/jmk.v7i1.39715

Orman, H. (2012). Towards a semantics of phish. *IEEE Symposium on Security and Privacy*, 91–96. https://doi.org/10.1109/SPW.2012.12

Searle, J. R. (1979). *Expression and meaning: Studies in the theory of speech acts*. Cambridge: Cambridge University Press.

Searle, J. R. (1994). Structure and Intention in Language: A Reply to Knapp and Michaels. *New Literary History*, *25*(3), 677–692. https://doi.org/10.2307/469472

Shafqat, W., Lee, S., Malik, S., Kim, H.-C. (2016). The language of deceivers: Linguistic features of crowdfunding scams. *Proceedings of the 25th International Conference Companion on World Wide Web (WWW '16 Companion)*, 145–150.

https://doi.org/10.1145/2872518.2889356

Sweller, J. (2011). Cognitive load theory. In B. H. Mestre, J. P.; Ross (Ed.), *The psychology of learning and motivation: Cognition in education* (pp. 37–76). Elsevier Academic Press. https://doi.org/10.1016/B978-0-12-387691-1.00002-8

Tian, C. A., Jensen, M. L., & Bott, R. (2024). The influence of affective processing on phishing susceptibility. European Journal of Information Systems. *Journal of Information Systems*, *34*(3), 460–474. https://doi.org/10.1080/0960085X.2024.2351442

Tyler, T. R., & Jackson, J. (2014). Popular legitimacy and the exercise of legal authority: motivating compliance, cooperation and engagement. *Psychology, Public Policy and Law*, *20*(1), 78–95. https://doi.org/10.1037/A0034514

Varekamp, I. (2014). Analyseren bij descriptief onderzoek: Ordenen, samenvatten, vergelijken, interpreteren. *KWALON*, *19*(3). https://doi.org/10.5117/2014.019.003.079

Wright, A., Hickman, T. T., McCoy, A. B., & Gadd, C. S. (2016). The Big Phish: Cyberattacks Against U.S. Healthcare Systems. *Journal of General Internal Medicine*, *31*(10), 1115–1118. https://doi.org/10.1007/S11606-016-3741-Z

Zhu, M., Yang, Y., & Hsee, C. K. (2018). The Mere Urgency Effect. *Journal of Consumer Research*, *45*(3), 673–690. https://doi.org/https://www.jstor.org/stable/27030212