Analysis of Practs and Allopracts in Typical Email Scams

Ifunanya Laurencia Ebekue, PhD
Department of English Language and Literature
Nnamdi Azikiwe University, Awka, Nigeria
li.ebekue@unizik.edu.ng
&
Ogechukwu Bridget Okeke
Department of English Language and Literature
Nnamdi Azikiwe University, Awka, Nigeria
bo.okeke@unizik.edu.ng

Abstract

Email scams continue to pose a significant threat to cyber security by exploiting users' trust through deceptive communication that imitates legitimate institutional messages. While prior research has predominantly focused on technical defences and psychological manipulation, there is a notable gap in understanding the pragmatic mechanisms scammers use to craft persuasive and deceptive emails. This study addresses this gap by applying Jacob Mey's Pragmatic Act theory to analyse the pragmatic acts (practs) and their linguistic variations (allopracts) commonly employed in email scams. Through qualitative discourse analysis of a diverse corpus of phishing messages, this research identifies how scammers strategically deploy practs such as warnings, requests, and promises within socially recognised communication patterns -pragmemes to increase message credibility and pressure recipients into compliance. The objectives are threefold: to categorise the common practs and allopracts in typical email scams, to examine how these acts replicate trusted institutional and social pragmemes, and to assess how raising awareness of these pragmatic strategies can enhance users' ability to detect email scam (phishing) attempts. The findings demonstrate that email scams systematically manipulate pragmatic norms to appear authentic, revealing the essential role of pragmatic competence in recognising and resisting such threats. This study contributes a novel linguistic

perspective to email scams research and offers practical implications for cyber security education, suggesting that enhancing pragmatic awareness among users can improve their defences against email scam (phishing) attacks and strengthen overall cyber resilience.

Keywords: Email scams, practs, allopracts, pragmemes, Pragmatic Act theory, linguistic deception, cyber security awareness

Introduction

Email scams represent a growing cyber security challenge, with millions of users worldwide falling victim to fraudulent schemes that exploit trust and communication norms. These deceptive emails typically impersonate legitimate entities such as banks, online retailers, or government agencies, aiming to manipulate recipients into disclosing sensitive personal information or performing actions that compromise their security (Verizon, 2023). Despite improvements in spam detection technologies such as spam filters and anti-phishing tools, email scams remain alarmingly effective. Their continued success is not solely attributable to technological loopholes but, more crucially, to scammers' ability to manipulate the communicative expectations and behaviours of their targets.

Language plays a central role in this manipulation. Scammers craft their messages with careful attention to linguistic style, tone, and structure in ways that convincingly simulate authentic communication. Beyond the literal meanings of words, these emails draw on deeper communicative strategies that exploit the social and contextual functions of language. As Mey (2001) emphasises, communication is not merely about the literal meaning of words but

involves pragmatic acts that are contextually embedded social actions, performed through language.

These practs, such as warnings, requests, threats, or promises, are realised in various surface forms known as allopracts, which adapt to specific communicative situations and cultural expectations. Email scams deploy such pragmatic acts (practs) and their linguistic variants (allopracts) in ways that activate familiar social scripts or pragmemes, that is, socially and culturally conventionalised communication patterns that guide interpretation and response. By mimicking institutional voices and aligning their messages with expected communicative routines, for example, bank notifications, password reset prompts, or fraud alerts, scammers increase the perceived legitimacy of their requests. This exploitation of pragmatic competence - the ability to interpret and use language appropriately within social contexts, creates a compelling illusion of authenticity.

To explore how these strategies function, this study applies Jacob Mey's Pragmatic Act Theory (Mey, 2001) to analyse the structure and intent of phishing emails. The theory provides a valuable lens for dissecting the interplay between linguistic form, pragmatic function, and contextual interpretation. According to Mey (2001), practs such as warnings, requests, and promises do not occur in a vacuum; they are embedded in recognisable cultural and institutional contexts and are realised through a variety of allopractic expressions. Understanding how phishing messages deploy these pragmatic resources can illuminate the techniques used to manipulate recipients and gain compliance.

The objectives of this research are threefold: first, to identify the predominant practs used in email scams; second, to analyse their

allopractic variations; and third, to examine how these pragmatic acts function within specific pragmemes to increase message credibility and victim compliance. To guide this inquiry, the study addresses the following research questions:

- What types of practs and allopracts are most commonly employed by scammers in typical email scams?
- How do these practs and allopracts replicate trusted institutional and social pragmemes?
- In what ways can awareness of these pragmatic patterns improve users' ability to detect email scam attempts?

By situating email scams within the framework of pragmatic acts, this study seeks not only to contribute to a theoretical understanding of language use in deceptive communication but also to offer practical insights for digital literacy and cyber security awareness initiatives. Enhancing users' pragmatic competence through awareness of these patterns may empower them to more critically evaluate suspicious emails, thereby reducing the effectiveness of scam tactics and strengthening collective cyber resilience.

Statement of the Problem

Despite growing awareness and advances in cyber security technologies, phishing emails remain a persistent threat in the digital age, not only due to technological sophistication but also because of the linguistic and communicative strategies they employ. While considerable research attention has been given to the technical, psychological, and sociological dimensions of phishing (Jacobsson & Myers, 2007; Baki & Zaqout, 2020), there remains a significant gap in understanding the pragmatic mechanisms that underpin the success of these fraudulent messages.

Email scammers do more than imitate the visual and structural elements of legitimate correspondence; they manipulate pragmatic acts such as warnings, promises, and requests to communicate behaviours. These acts, referred to by Mey (2001) as practs, and their linguistic variations as allopracts, function within culturally established pragmemes that guide interpretation and response. However, the deployment of these pragmatic tools in phishing contexts remains underexplored in current scholarship. This lack of focus on the pragmatic dimension of phishing represents a significant gap in understanding how scammers exploit users' pragmatic competence - the ability to interpret language appropriately in context to achieve deception. Without insight into how practs and allopracts are strategically embedded in phishing messages, both academic inquiry and cyber security education may fail to fully equip users to detect and resist such threats. Addressing this problem calls for a pragmatic analysis of phishing emails grounded in Mey's Pragmatic Act Theory (2001).

Significance of the Study

This study offers both theoretical and practical contributions. Theoretically, it advances the application of Mey's Pragmatic Act Theory (Mey, 2001) by exploring how practs and allopracts function in deceptive email communication. It highlights the role of pragmemes in shaping the linguistic strategies that scammers use to exploit trust and simulate authentic interactions. This contributes to the growing body of research in digital pragmatics and contextual meaning-making in online discourse.

Practically, the study provides insights that can support cyber security awareness efforts by identifying the pragmatic features that make phishing emails persuasive. Understanding these strategies can help

improve users' pragmatic competence, equipping them to better detect and resist fraudulent messages. By bridging linguistic theory and cyber security practice, the research underscores the importance of interdisciplinary approaches to combating digital threats. The study also provides critical insights for cyber security education. By uncovering how practs and allopracts are used to exploit familiar pragmemes, the research enhances understanding of the linguistic strategies behind phishing emails. This knowledge can inform the development of training programmes that foster pragmatic competence, that is, the ability to detect communicative patterns and evaluate communicative authenticity.

Furthermore, the study bridges the gap between linguistics and cyber security, offering an interdisciplinary approach that moves beyond surface-level analysis and highlights the importance of context, culture, and communication norms in phishing detection. It empowers users to be more sceptical of familiar-sounding emails and builds capacity for critical engagement with online messages, ultimately contributing to stronger individual and collective cyber resilience.

Scope of the Study

This study is limited to the linguistic and pragmatic analysis of typical email scam messages, with particular focus on the deployment of practs and allopracts as defined within Mey's Pragmatic Act Theory (Mey, 2001). It does not address the technical infrastructure or psychological profiling behind scam creation but concentrates on how scammers use language pragmatically to imitate legitimate communication and manipulate recipients.

The data for this study consist of authentic email scams gathered from publicly available scam message repositories, cyber security forums,

and individual contributions. These emails are analysed for the pragmatic acts they perform, such as requests, threats, offers, or warnings, as well as the allopractic variations that reflect different scam strategies and target different social or institutional pragmemes.

Geographically, the study does not limit itself to a specific region but focuses on globally circulated scam emails written in English. This scope allows for the identification of widely used pragmatic strategies that transcend cultural and national boundaries while still reflecting specific communicative norms.

By concentrating on the pragmatic features of language in email scams, this study aims to contribute to both linguistic theory, particularly in the areas of digital pragmatics and cyber communication, and to cyber security awareness efforts aimed at improving users' resistance to phishing attacks. Technical, psychological, and purely semantic analyses fall outside the scope of this study.

Conceptual Framework

This study draws on Jacob Mey's (2001) Pragmatic Act theory to explore the linguistic and social mechanisms employed in email scams and phishing, situated within the broader context of cyber security. The framework revolves around three core concepts - practs, allopracts, and pragmemes while also situating the study within the practical phenomena of scams, phishing, and cyber security awareness. These concepts together illuminate how scammers use language pragmatically to deceive victims.

Scams, Email Scams and Phishing

A scam is an intentional attempt to deceive or defraud individuals, often for financial or personal gain. Email scams are a form of digital fraud that uses deceptive messages to manipulate recipients into revealing personal information, clicking malicious links, or taking actions that compromise security. Phishing, a prevalent type of email scam, is defined by Encyclopaedia Britannica as "an act of sending e-mail that purports to be from a reputable source … and that seeks to acquire personal or financial information" (Britannica Editors, 2025). IBM (2024) further explains that phishing is a cyberattack where attackers use fraudulent communications to trick victims into revealing sensitive information. These definitions situate phishing and email scams as cybersecurity threats that exploit human behaviour and trust.

Cyber Security Context

Cyber security is the practice of protecting systems, networks, and data from digital threats, including phishing and other scams. The UK's National Cyber Security Centre (NCSC, n.d.) defines it as the measures that help individuals and organisations reduce the risk and impact of cyberattacks. According to TechTarget, cyber security involves "defending systems, networks, and data against digital threats and unauthorised access" (Yasar et al., 2025). Effective cyber security therefore requires not only technical measures but also awareness of the linguistic and pragmatic strategies scammers use to deceive users.

Practs: Pragmatic Acts as Social Actions

Practs are the fundamental communicative actions performed through language in social interactions. According to Mey (2001), "pragmatic acts are intentional actions done by speakers to affect the behavior or

beliefs of hearers" (22). These acts include warnings, requests, promises, threats, and other social moves that go beyond mere utterances to perform an action in context. In email scams, practs are central to driving recipients toward a desired behaviour, such as clicking a malicious link or providing personal information. For example, an email scam may issue a warning of account suspension, a request for password confirmation, or a promise of a financial reward. Each of these acts is designed to provoke urgency, fear, or desire, which scammers exploit to manipulate victims.

Allopracts: Variations of Practs

Mey (2001) introduces the concept of allopracts to capture the diverse linguistic forms that can realize a single pragmatic act. Mey (2001) explains that "every pract is at the same time an allopract, that is to say, a concrete instantiation of a particular pragmeme" (2001:221). "Allopracts are the alternative linguistic manifestations of a given pract, shaped by factors such as context, speaker intention, and cultural norms" (36). For instance, a request can be direct - "Please confirm your password now" or indirect - "We would appreciate your prompt attention to this matter".

In email scam contexts, scammers carefully choose allopracts to maximize persuasiveness and avoid immediate suspicion. They may alternate between formal, authoritative language mimicking official institutions and informal, urgent tones that induce panic. These variations contribute to the deceptive effectiveness of the message.

Pragmemes: Social Scripts Guiding Interpretation

Pragmemes are culturally entrenched communicative patterns that shape how messages are interpreted and responded to. Mey (2001) defines pragmemes as "socially conventionalised pragmatic acts that

are recognised and expected within particular social contexts" (37). Mey (2001) notes that "the central part in the concept of 'pragmatic act' is pragmeme. A pragmeme is the generalised pragmatic act; it is regarded as an abstraction" (221–222). Pragmemes provide the social and cultural framework in which practs and allopracts are realised, ensuring that individual acts are interpreted predictably.

Pragmemes embed knowledge about roles, expectations, and typical behaviours in interactions, such as those between customers and banks or employers and employees. Email scammers exploit well-known pragmemes, such as official banking alerts or delivery service notifications to create plausible and compelling messages. They exploit these templates by aligning fraudulent messages with these recognised patterns, increasing perceived legitimacy (Mey, 2001: 221–222; Ugoala & Israel, 2020). Pragmemes allow for variation and flexibility, enabling scammers to modify tone, urgency, or formality while operating within recognisable social scripts. Understanding pragmemes separately from practs and allopracts helps users detect underlying manipulative patterns in phishing emails.

Application: Interplay of Practs, Allopracts, and Pragmemes in Email Scams

In phishing and email scams, scammers deploy practs through varied allopracts that fit within established pragmemes associated with trusted institutions. For instance, a warning about "suspicious activity", a pract may be expressed formally or urgently in different allopracts within a bank-customer pragmeme. Mey (2001) highlights that pragmatic force is central: "there is only one force in any act of uttering … and it is pragmatic, the force of the pragmeme" (as cited in Ugoala & Israel, 2020: 3). By understanding this interplay, users can develop pragmatic competence, the ability to recognise deviations

from genuine communication patterns and resist manipulative messages, complementing cyber security awareness.

Theoretical Framework: Mey's Pragmatic Act theory

This study adopts Mey's Pragmatic Act Theory as its theoretical framework. This theory was developed by Jacob L. Mey in 2001. Pragmatic Act Theory emphasises the contextual nature of language use, focusing not just on what is said but on what is done with language in real-world social settings. It recognises that language is not a static structure but a dynamic tool for performing actions within particular cultural and communicative contexts. At the core of this theory is the notion of the pragmeme. A pragmeme is a generalized pragmatic act that encompasses both the linguistic form and the contextual conditions of its use. Each pragmeme is realised in actual communication as a pract, and these practs can vary depending on the socio-pragmatic situation, resulting in multiple allopracts. For example, a scam email designed to deceive a recipient may manifest as a formal business proposal, a desperate plea from a fabricated royal figure, or a notification of a fabricated financial windfall. These are all distinct allopracts of the same underlying deceptive pragmeme.

To strengthen the theoretical rigour of this study, it is also essential to consider Mey's later elaboration of the three levels of pragmemes: micro-pragmemes, meso-pragmemes, and macro-pragmemes. Micro-pragmemes refer to localised, everyday small-scale pragmatic acts that occur in interpersonal interactions, such as greeting, requesting, apologising, thanking, promising, and so on. These operate as specific utterances within an email. Meso-pragmemes reflect professional, institutional, or community-based pragmatic acts governed by social roles, group expectations, and professional norms, such as instruction, directive, invocation, prescription, and announcement. They usually

occur within classroom contexts (e.g., 'turn to page 23 of your textbook'), church contexts (e.g., 'let us pray'), hospital contexts ('take your drugs twice a day'), and office contexts ('schedule a meeting for tomorrow'). These operate at the level of the email genre or structure in the form of typical moves in scam messages such as "Click here to confirm your identity". Macro-pragmemes represent broader societal-level pragmatic acts that express or enact dominant ideologies, collective beliefs, and power structures through language. These function to legitimise authority, mobilise national identity, naturalise ideology, and manufacture public consent. They appear mostly in media headlines, political speeches, religious sermons, and so on. Email scammers operate at this level, embedding and exploiting societal ideologies, collective beliefs, and global narratives to manipulate their victims. These may take the form of impersonating financial institutions, the UN, IMF, or World Bank, for example: "Your account is at risk. Click here to rectify the issue"; "This is to notify you that the World Bank payment unit …". They can also take the form of appeals to humanitarian ideals such as "Help donate to orphans and widows" or beliefs in upward mobility through luck or foreign aid, as in "You have been selected to manage the African Trust Fund".

Email scams typically engage all three levels simultaneously. A single scam email may use a micro-pract to request bank information (micro-pragmeme), embed this in a culturally familiar narrative (meso-pragmeme), and appeal to larger ideological assumptions about wealth, poverty, or benevolence (macro-pragmeme). This layered deployment increases the plausibility and emotional appeal of the scam, thereby enhancing its persuasive power. The choice of Mey's Pragmatic Act Theory is therefore both appropriate and methodologically strategic. It allows the researchers to account for

contextual variability, linguistic diversity, and cultural specificity in scam discourse. It also provides tools to examine how scammers adapt their language pragmatically through multiple practs and allopracts, and how they exploit common cultural narratives and discourse frames to manipulate victims' expectations and emotions.

By examining scam emails through the lens of micro-, meso-, and macro-pragmemes, this study captures the complex pragmatic layering that characterises deceptive online communication. This detailed approach not only enriches our understanding of digital fraud tactics, but also contributes to the growing field of digital pragmatics and cyber communication.

Empirical Review

Email scams have attracted significant attention from cybersecurity, psychology, and linguistics researchers. Jakobsson and Myers (2007) offered an early comprehensive taxonomy of phishing, focusing on the technical and behavioural aspects of these attacks. Their framework primarily addressed the methods and motives behind phishing but did not examine the pragmatic or linguistic strategies scammers use in crafting deceptive messages.

Linguistic analyses of phishing emails have explored stylistic and lexical features that mark phishing attempts. Baki, Al-Samarraie, and Zaqout (2020) analysed phishing corpora to identify common linguistic markers such as urgency cues, threats, and impersonation tactics. However, their work mainly described surface features without explicitly linking them to underlying pragmatic theories.

Felt et al. (2012) studied the impact of security warnings on user behaviour, relying on cognitive and behavioural theories to explain

attention and comprehension. While informative about psychological reactions, this study did not explore the pragmatic functions of language in phishing messages.

In the realm of pragmatics and discourse analysis, Khosravani and Shokri (2017) applied pragmatic analysis to social engineering attacks, using relevance theory and Gricean maxims to understand how deceptive language exploits social expectations. Their work illuminated how pragmatic violations can function as manipulation but was limited to face-to-face or telephone interactions rather than written phishing emails.

Additionally, researchers such as Flowerdew (2013) and Rock (2014) have used discourse analysis frameworks to analyse institutional emails, highlighting how power, politeness, and social roles shape communication. These frameworks offer tools to examine how phishing emails imitate institutional discourse but do not explicitly apply Pragmatic Act Theory.

The theoretical frameworks used in these studies range from cognitive psychology (Felt et al., 2012), relevance theory (Khosravani & Shokri, 2017), discourse analysis (Flowerdew, 2013), to social engineering models (Jakobsson & Myers, 2007). While valuable, none fully integrates Mey's (2001) Pragmatic Act Theory to analyse how phishing emails pragmatically enact social actions through practs, allopracts, and pragmemes.

This study differs by explicitly employing Mey's (2001) Pragmatic Act Theory as its analytical lens to:

- Systematically identify and categorise practs (pragmatic acts) and allopracts (their linguistic variants) in email scams.

- Examine how these pragmatic acts are embedded within culturally and institutionally recognised pragmemes (social scripts), which scammers exploit to simulate trustworthiness.
- Bridge linguistic pragmatics and cybersecurity research, offering a novel interdisciplinary approach to understanding phishing beyond surface linguistic features or psychological effects.
- Provide practical implications by highlighting how improving pragmatic competence can enhance users' ability to detect phishing scams.

By focusing on the pragmatic dimension of phishing communication, this study contributes fresh theoretical and empirical insights that advance both linguistic pragmatics and cybersecurity education.

Methodology

This study adopts a qualitative research design, drawing on discourse and pragmatic analysis to explore the pragmatic acts (practs) and their linguistic variants (allopracts) employed in email scams. Guided by Mey's Pragmatic Act Theory (2001), the study examines how scammers strategically deploy these acts within familiar social communication scripts, referred to as pragmemes, to manipulate and deceive recipients.

The primary instrument for data collection was a request for voluntary submission of scam emails, disseminated through a WhatsApp group comprising university students and colleagues. Participants were invited to forward scam emails they had personally received to the researcher for academic analysis. Only emails that participants had already identified as scams were submitted. No personal data, email addresses, or identifying information were collected or analysed.

In addition to WhatsApp submissions, supplementary data were obtained from publicly accessible cyber security repositories and scam-reporting platforms, including PhishTank, Spamhaus, and user-submitted scam archives hosted on cyber security awareness websites. These platforms were used to augment the dataset and ensure diversity in scam types and linguistic patterns.

The final dataset consisted of a purposive sample of 30 authentic email scams, collected within the six months preceding the study. The emails were selected to represent common scam categories such as financial fraud, account verification requests, and reward or lottery scams, ensuring a broad range of pragmatic acts and linguistic realisations.

The analysis was conducted in several stages. First, each email was examined to identify the dominant pragmatic act, such as warnings, requests, promises, or threats, in accordance with Mey's definitions (Mey, 2001:22). Next, the various linguistic forms through which these acts were realised - the allopracts were categorised by analysing features such as tone, modality, directness, and politeness strategies (Mey, 2001:36).

Subsequently, the identified practs and allopracts were mapped onto relevant pragmemes - socially recognised communicative scripts such as bank notifications or official service alerts which scammers imitate to enhance message credibility (Mey, 2001: 37).

This methodological approach enables an in-depth understanding of the pragmatic strategies underlying email scams and provides practical insights into how users' pragmatic competence can

be strengthened to improve the detection of, and resistance to, such scams.

Data Analysis

The table below presents selected samples of email scams analysed in this study. The samples were purposively selected from the collected dataset to illustrate how pragmatic acts (practs), their linguistic variants (allopracts), and pragmemes operate in phishing and scam emails. The analysis follows Mey's Pragmatic Act Theory (2001) and is presented for clarity and ease of understanding.

Table 1: Pragmatic Analysis of Email Scams: Pragmeme, Practs and Allopracts

S/N	Scam Type	Sample Extract	Pragmeme (Social Script Exploited)	Pract	Allopracts (Variants)	Pragmatic Interpretation
1	Account suspension warning	Dear Customer, Your account has been suspended due to suspicious activity. Please click the link below to verify your identity and restore access immediately."	Institutional security alert pragmeme	Warning	Your account has been temporarily locked; Your account access is disabled	The message functions as a warning that creates urgency and fear. By mimicking official account security notifications, the scammer exploits recipients' expectations of legitimate

						institutional alerts, prompting immediate action.
2	Prize notification scam	Congratulations! You have won a $1,000 gift card. To claim your prize, please provide your full name, address, and credit card details.	Reward solicitation pragmeme	Promise / Offer	You're the lucky winner; "Claim your cash reward now	The promise of a reward serves as positive reinforcement, enticing recipients to disclose personal information by exploiting familiar social scripts surrounding prizes and sweepstakes.
3	Delivery failure notification	Your package could not be delivered. Please confirm your shipping address by clicking the link below to avoid return of your parcel.	Delivery notification pragmeme	Request for confirmation	Delivery attempt failed. Update your address; Important: Delivery issue detected	The email requests action to prevent a negative outcome. By imitating courier service notifications, it exploits users' expectations of legitimate delivery communications.
4	Fake bank alert	Important: Your bank account has unusual activity. Confirm	Financial security alert pragmeme	Warning	Unauthorized withdrawal detected; Suspiciou	The warning exploits trust in financial institutions

		your recent transactions by logging into your account through the secure portal.			s charges noticed	and urgency associated with protecting one's finances, prompting recipients to interact with fraudulent links.
5	Tax refund scam	The IRS has issued a tax refund for you. Submit your Social Security Number and bank details here to receive your payment.	Government refund notification pragmeme	Promise / Request	Tax refund pending; You qualify for a refund	This scam combines promises and requests, exploiting expectations of official government communication about financial refunds to elicit sensitive data.
6	Invoice payment scam	Dear Vendor, Please find attached the invoice for your recent services. Confirm receipt and remit payment to the account specified.	Commercial transaction notification pragmeme	Request	Invoice attached for your review; Payment overdue	The email imitates routine business communication, relying on established commercial practices to induce payment or deliver malware through attachments.
7	Social media account	Your social media account has been	Social media security alert pragmeme	Warning / Request	Unusual login activity detected;	The message exploits users'

	verification	flagged for suspicious behaviour. Verify your account now to avoid suspension.			Immediate verification required	concern for account security and continuity of access, prompting compliance with verification requests.
8	Tech support fraud	Your computer has been infected with a virus. Call our support team immediately to resolve this issue.	Technical support alert pragmeme	Warning / Request	Malware detected; System alert: Your PC is at risk	By invoking fear of technical failure or data loss, the scammer manipulates users into contacting fraudulent support services.
9	Charity donation scam	Support disaster relief by donating today. Click here to make a secure donation and receive a tax receipt.	Charitable solicitation pragmeme	Request	Help families affected by floods; "Your generosity can save lives	The request appeals to altruism and social responsibility, exploiting norms surrounding charitable giving during crises.
10	Package delivery alert	Your package could not be delivered. Please confirm your shipping address by clicking the link below.	Package delivery notification pragmeme	Request	Update your address promptly; Delivery issue detected	The scam relies on familiar delivery alert formats to elicit personal information or redirect users to phishing websites.

The analysed email scam samples demonstrate that practs, such as warnings, requests, and promises, are strategically aligned with social expectations. Allopracts serve as variations in phrasing that adapt to different targets while preserving the underlying pragmatic function. Pragmemes operate as familiar institutional or social communicative acts that establish legitimacy and prompt compliance. These examples illustrate that email scams are carefully constructed pragmatic acts embedded within culturally recognised social scripts. The manipulation of practs and allopracts within established pragmemes not only disguises deceptive intent but also exploits users' reliance on familiar communication patterns to facilitate compliance.

This evidence supports Mey's (2001) view that pragmatic acts are embedded within cultural and social contexts, and that scammers exploit recognised pragmemes to deceive effectively. A pragmatic perspective deepens understanding of phishing as a form of social engineering grounded in pragmatic competence and cultural norms. It further validates Mey's assertion that communication is a dynamic, contextually situated act, with pragmatic acts serving as key units of meaning and function.

Discussion

The findings of this study illuminate the sophisticated pragmatic strategies scammers employ in phishing emails, particularly through the use of practs and allopracts within established pragmemes. The consistent deployment of warnings, requests, and promises aligns closely with Mey's (2001) Pragmatic Act Theory, which emphasises how communicative acts go beyond literal meaning to perform social functions.

Warnings in phishing emails exploit urgency and threat to provoke immediate compliance. This mirrors real-world institutional communications, such as bank alerts, where time-sensitive warnings are common (Mey, 2001: 22). The use of direct and forceful allopracts demonstrates scammers' awareness of the need to bypass reflective reasoning, leveraging emotional triggers such as fear to undermine recipients' scepticism.

Requests varied from polite and indirect to commanding forms, indicating an adaptive approach tailored to perceived social distance and trust levels. This variation reflects Mey's concept of allopracts as multiple linguistic realisations of the same pragmatic act (Mey, 2001: 36–38). By mimicking the tone and style of legitimate institutions, scammers enhance the perceived authenticity of their messages, making detection more difficult.

Promises, although less frequent, function as positive reinforcement within the pragmemes of reward and benefit. These acts draw on social expectations of reciprocity and gain, which phishing scammers manipulate to entice victims. The integration of promises into phishing pragmemes reveals a layered strategy that combines fear and hope to increase effectiveness.

Mapping practs and allopracts onto pragmemes demonstrated how scammers replicate culturally and institutionally familiar social scripts. This confirms Mey's argument that pragmemes guide expectations and interpretations in communication (Mey, 2001:37). The ability of scammers to exploit these shared scripts highlights a critical vulnerability in users' pragmatic competence.

This study fills a significant gap in phishing research by applying a detailed pragmatic framework rather than focusing solely on technical or psychological aspects. It underscores the importance of pragmatic awareness in cyber security education, suggesting that training users to recognise these pragmatic acts and their variants can improve detection and resistance to phishing.

From the foregoing, the pragmatic act perspective provides a valuable lens for understanding email scam strategies, advancing both theoretical linguistics and practical cyber security measures. Future research could explore pragmatic competence training and its impact on phishing susceptibility.

Conclusion

This study has demonstrated that phishing emails strategically employ pragmatic acts (practs) and their linguistic variants (allopracts) within culturally recognized pragmemes to manipulate recipients into compliance. By applying Mey's Pragmatic Act theory (2001), the study has revealed how warnings, requests, and promises function as key communicative tools scammers use to mimic trusted institutional communications and exploit users' pragmatic expectations.

The analysis highlights that phishing success is not merely a result of technical trickery but also deeply rooted in linguistic and social interaction strategies. Understanding these pragmatic dimensions enriches the theoretical discourse on phishing and offers practical avenues for enhancing cyber security awareness. Specifically, developing users' pragmatic competence - awareness of how language functions in social contexts can empower individuals to critically evaluate suspicious messages and reduce victimization.

In conclusion, recognising phishing emails as pragmatic acts embedded within social communication patterns shifts the focus from purely technical solutions to a more holistic understanding of human communication vulnerabilities. This approach not only enriches academic inquiry but also holds promise for practical defense against increasingly sophisticated cyber threats.

References

Baki, R., Al-Samarraie, H., & Zaqout, F. (2020). Phishing attacks: A Taxonomy and Future *Directions. Journal of Network and Computer Applications,* 102, 164–174. https://doi.org/10.1016/j.jnca.2017.12.002

Britannica Editors. (2025). *Phishing. Encyclopaedia Britannica.* https://www.britannica.com/technology/phishing

Felt, A. P., Chin, E., Hanna, S., Song, D., & Wagner, D. (2012). Android permissions: User Attention, Comprehension, and Behavior. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (SOUPS '12) (Article 3). https://doi.org/10.1145/2335356.2335360

Flowerdew, J. (2013). *Discourse in English Language Education*. Routledge.

IBM. (2024). What is Phishing? https://www.ibm.com/think/topics/phishing

Jakobsson, M., & Myers, S. (2007). Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft. *Wiley-Interscience*.

Khosravani, M., & Shokri, H. (2017). Pragmatic Analysis of Deceptive Language in Social Engineering. *Journal of Pragmatics*, 115, 55–69. https://doi.org/10.1016/j.pragma.2017.04.002

Mey, J. L. (2001). *Pragmatics: An Introduction* (2nd ed.). Wiley-Blackwell.

National Cyber Security Centre. (n.d.). What is Cyber Security? https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security

Rock, F. (2014). Institutional Discourse. In T. A. van Dijk (Ed.), *The Handbook of Discourse Analysis, PP. 344 - 363,* Wiley-Blackwell

Ugoala, C. N., & Israel, E. O. (2020). Pragmatics and Discourse Analysis. *Open Journal of Modern Linguistics*, 10(3), 1–15. https://www.scirp.org/pdf/ojml_2020112413581619.pdf

Verizon. (2023). Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/

Yasar, K., Shea, S., & Gillis, A. S. (2025). Cybersecurity Definition. TechTarget. https://www.techtarget.com/searchsecurity/definition/cybersecurity