Journal of English Language Teaching and Applied Linguistics
ISSN: 2707-756X
DOI: 10.32996/jeltal
Journal Homepage: www.al-kindipublisher.com/index.php/jeltal

JELTAL
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Real or Reel: A Comparative Analysis of Authentic and Phishing Emails

Julysa C. Cardona
PhD Student, Department of English, Mindanao State University-Iligan Institute of Technology, Iligan City, 9200, Philippines
Assistant Professor, Language and Letters Department, Bukidnon State University, Malaybalay City, Bukidnon, 8700 Philippines
Corresponding Author: Julysa C. Cardona, **E-mail**: julysacardona@buksu.edu.ph

| ABSTRACT

Although technology can be used for good reasons, the same can be exploited by cybercriminals for malicious intents and activities like phishing attacks. The use of phishing emails in such crimes makes it riveting to understand language's role in such a deceptive undertaking. Hence, this qualitative work comparatively analyzed the language correctness and deviations, illocutionary speech acts, and persuasion principles of phishing and authentic emails to draw the line that separates the genuine from the copycat. The results reveal that although phishing emails commit more types of language deviations relating to parallelism, pluralization, preposition usage, subject-verb agreement, sentence fragments, and possessive form, there are also instances of faulty use of punctuation markers in authentic emails, thereby making it unreliable to judge an email's veracity through language correctness or deviations alone. Moreover, the simultaneous use of expressive, directive, and representative acts was found in phishing and authentic emails, while the former has added the commissive act through subtle threats. Also, authority was typical in both phishing and authentic emails, while the former employs other persuasion principles such as reciprocity, social proof, and liking, indicating that phishers not only impersonate legitimate institutions but also stimulate the victims' emotions. Finally, this study draws that what sets a real email apart from the reeling one is not mainly the correctness or the deviations in an email's language, but rather, it is the phishing email's tendency to evoke feelings of fear and a sense of urgency behind the text that may give their dishonesty away.

| KEYWORDS

Phishing Emails, Authentic Emails, Language Correctness, Language Deviations, Illocutionary Acts, Persuasion Principles

| ARTICLE INFORMATION

ACCEPTED: 01 February 2025 **PUBLISHED:** 22 February 2025 **DOI:** 10.32996/jeltal.2025.7.1.15

1. Introduction

Today's world has led people to more frequent digital engagements and activities. With a few taps on the screen, one can shop from digital stores, book a ride to avoid the hassle of commuting, or even move money from one bank to another. The digital space, however, presents not only mere connectivity and convenience. Danger, harm, and crimes have also made their way into cyberspace through hacking, malware, and phishing attacks (Singer & Friedman, 2014).

In the Philippines, statistics on internet attacks show that phishing, a form of online manipulation that tricks susceptible users into providing sensitive information, is considered the top cybercrime committed in the country during the COVID-19 pandemic followed by online selling scams and the spread of fake news (Asani et al., 2021; Hani, 2021). In 2021, 1.34 million phishing attacks were detected in the whole year, but in the first half of 2022 alone, over 1.8 million attacks have been identified (Statista, 2022). The increasing instances of these cybercrimes in the Philippines speak of the economic risks and social dangers the vulnerable population may face, thereby prompting the government to bolster the country's cyber security.

One specific type of phishing attack involves the use of phishing emails. In this cybercrime, attackers masquerade as trustworthy sources, then send out fake emails to steal people's sensitive information such as usernames and passwords (Rawat & Kunwar,

2023; Alam et al., 2020; Chowdhary et al., 2024). This fundamental knowledge of phishing mechanisms reveals that not all emails are real. Rather, some emails reel possible victims into the phishing trap, causing financial loss and identity theft. The damaging impact of this loss underscores the need to explore various cyber harms and the ways to deter them. In the context of phishing attacks, one area of interest may be the exploration of how phishing emails capitalize on the power of language given that it plays a crucial part in manipulating and deceiving phishing victims (Brooks, 2018; Chen, 2021; Hazra & Majumder, 2024). Phishers, imitating legitimate entities, employ persuasive language in their fake emails to establish a sense of urgency or legitimacy.

Considering the influential role that language plays in proliferating cyber-attacks like phishing, this present work aimed at comparing fake and genuine bank emails in terms of their linguistic elements specifically (a) language correctness and deviations, (b) illocutionary acts, and (c) persuasion principles.

Language correctness refers to a linguistic form's adherence to the grammatical, syntactical, and stylistic norms of a language. It covers aspects like the proper use of grammar rules, punctuation, spelling, verb tense, subject-verb agreement, and overall clarity of expression (Murphy, 2019). More so, contextual appropriateness is essential for effective communication since inaccuracies may potentially cause misunderstandings (Larsen-Freeman, 2003; Swan, 2005). This means that the language choices of a conversation or written communication are influenced by the audience's background, culture, situation, purpose of communication, level of formality, or tone. Language deviations, on the other hand, encompass phonological, graphological, lexical, and grammatical deviations that break conventional linguistic norms to enhance creativity and persuasion (Budiharto, 2016; Yaghubyan, 2020). Comparing the language correctness and deviations between phishing and genuine emails may help identify common patterns that may serve as red flags for email recipients.

Another riveting aspect in comparing the language of phishing and genuine emails is the speech act. Originally developed by Austin (1962), this theory forwards the notion that there is something more than what the person says. A speech act is an utterance that renders a function in communication. A single utterance alone can carry out three different speech interpretations which can be categorized according to Searle (1969) as a locutionary act, an illocutionary act, and a perlocutionary act. The locutionary act refers to the literal meaning of the utterance, while the illocutionary act pertains to the speaker's communicative function. On the other hand, the perlocutionary act relates to the actual effects of the utterance on the hearers based primarily on their response.

Speech acts are Searle's (1969) way of classifying when the performance of an act may be appropriate or inappropriate. Hence, he focused on the illocutionary which performs five (5) types of acts such as representative, declarative, directive, expressive, and commissive. The representative act includes describing events or processes, stating, asserting, or claiming. The declarative act, however, includes pronouncing, sentencing, and christening, while the directive act covers commanding, requesting, pleading, and inviting. The expressive act involves greeting, scolding, condoling, appreciating, congratulating, apologizing, and thanking, while the commissive acts are those that are betting, challenging, promising, threatening, offering, vowing, and warning. In the context of phishing emails, these speech acts may be utilized by impersonators in an attempt to deceive and persuade their victims. Hence, comparing the speech acts of phishing and genuine emails can reveal how phishers make the most out of a language's function to deceive the recipients.

Finally, this study also looked into the principles of persuasion depicted within both phishing and genuine emails. Cialdini (1984) discusses six (6) key principles of persuasion. These principles are reciprocity, commitment and consistency, social proof, authority, liking, and scarcity. (1) The principle of reciprocity describes that people are more likely to accept a request out of feeling that they owe the person something. (2) Commitment and consistency talk about how people prefer to stick with their decisions and follow their usual beliefs and actions instead of changing their minds all the time. (3) Social proof means people often tend to trust something if they see some other people who have done or tried the same thing. (4) Authority refers to how people are more likely to believe individuals whom they perceive as credible experts. (5) Liking means people are more receptive to and are easily persuaded by those that they like and feel a connection with rather than by those they do not appreciate. Finally, (6) scarcity refers to the persuasion principle that when something is limited edition, rare, or scarce, people are more likely to desire it, thereby motivating them to take action. Exploring the persuasion principles employed in both phishing and genuine emails is beneficial in raising awareness of how language can be used to manipulate or deceive people, thereby enhancing deterrence from scams and fraud. In light of these goals, this paper sought to answer the following research questions:

1. What are the similarities and differences between phishing and authentic bank emails, specifically in terms of:
    a. language correctness and deviations;
    b. illocutionary speech acts; and
    c. persuasion principles?
2. How do these similarities and differences outline the linguistic cues that set apart real emails from the reeling ones?

2. Literature Review

The first instance of a phishing attack transpired in the mid-1990s when a group of hackers impersonated American Online (AOL), an internet service provider and web portal based in the United States, via instant messages and emails to steal people's passwords. Since then, phishing attacks have continued to cause havoc to vulnerable victims especially now that with the rise of modernization, cybercriminals have also been using more sophisticated techniques to reel their victims into the phishing trap (Proudfoot et al., 2011; Alkhalil et al., 2021; Priya et al., 2024).

The majority of phishing attacks are performed in a three-step process. First, the phishers gather the email addresses of their probable victims from sources like web pages and forums. Second, they send huge bulks of phishing emails impersonating official banking domains or authentic intuitions with the use of anonymous servers. Finally, they lure their recipients into a fake website through the attached hyperlinks (Chandrasekaran et al., 2006). Although phishing emails commonly contain links that lead the end-users to a fake website, other types of phishing emails do not contain any links but bank on the victim's curiosity by enticing them into replying with sensitive information (Aggarwal et al., 2014).

Although technology-based cyber security innovations have been developed and studied to combat phishing activities (Kim et al., 2014; Chen et al., 2014; Aksu et al., 2017; Baykara & Gürel, 2018; Pietrantonio et al., 2024), some authors argue that the blend of machine-based solutions and user awareness could still be the most effective countermeasure against cyber-attacks like phishing emails (Park et al., 2014; Kumar et al., 2023; Arévalo et al., 2023). This accentuates the need to educate people to manually distinguish the veracity of a text so they do not fall victim to the phishers' bait.

Brooks (2018) highlights that being able to manually recognize whether an email is real or fake is an important skill. She argues that every phishing email has an inherent tendency to employ persuasive strategies to successfully lure the victims in. Hence, she asserts that one's ability to identify how persuasion is carried out in deceptive texts may help combat the increasing cases of phishing scams. This proves that a study centered on the natural aspect of phishing emails can be beneficial in enhancing people's skill to manually detect fraud. Thus, this present work focuses on the linguistic aspects of both phishing and authentic emails to determine linguistic patterns that set the copycat apart from genuine ones.

Existing pieces of literature have demonstrated that since fake emails contain logos and text that may appear authentic, then an examination of language correctness cannot be used as a reliable means to pinpoint phishing attempts, thereby underscoring the need to semantically analyze malicious intents to deceive rather than to focus on language correctness (Blythe et al., 2011; Peng et al., 2018). Despite these contentions, more recent studies have argued that the use of poor language may serve as a red flag because, unlike legitimate communications which usually maintain higher standards of language correctness, phishing emails often display language issues related to improper capitalization and punctuation, misspellings and the like, implying that the email may be a hoax (Patel et al., 2024; Cardona, 2024). These differing views on the value that language correctness and deviations serve to potentially indicate a fake email from an authentic one imply two things. First, although language correctness and deviations may not fully draw the line by which the genuine and the fake converge, they can still describe the divergences between phishing and authentic emails, thereby making this aspect worthy of attention. Second, language correctness and deviations may bring vital insights into the understanding of the language of phishing and authentic emails when combined with semantic analysis. To address these gaps, this present work therefore takes the exploration further to not only language correctness and deviations but also the illocutionary acts and persuasion principles.

Studies have shown that emails perform various speech acts simultaneously as they reflect multiple communication intents (Carvalho, & Cohen; 2005, Chiluwa, 2010; Brooks, 2018). In à 2010 study, Chiluwa made use of the speech acts theory to explore the discourse strategies and functions found in 52 samples of fake emails in Nigeria. His study revealed that the sampled data employed speech acts such as expressive, representative, commissive, and directive acts. More specifically, the representative act was the most frequently used as the proposals are structured in the form of narratives, while the expressive act is utilized in the form of polite greetings to win the receiver's interest. The commissive act is used through unrealistic promises, while the directive act urges the receiver to act promptly. Relative to this work, Brooks (2018) also revealed that threats (commissive) and declaratives (performatives) are the common acts used in phishing emails, along with the use of prominent words to denote the phisher's superiority. On the other hand, an authentic professional email often involves speech acts like requests, commitments, and amendments, exhibits a formal greeting and closing, and avoids casual tones but rather maintains a respectful tone throughout the message (Carvalho, 2011; Malka et al., 2015; Unnam et al., 2019). Comparing the speech acts between phishing and authentic emails helps not only in describing the limitations of the language of imposters but also in understanding how phishers conceal their actual intent behind the communicative function of their message.

Rajivan and Gonzales (2018) posit that the success of phishing attacks depends on the effective exploitation of human weaknesses. Taking this into account, exploring how persuasion principles are employed in fake and authentic texts may reveal insights into

how deception takes place in phishing emails. Akbar (2014) conducted a quantitative analysis of the reported phishing emails between August 2013 and December 2013 in the Netherlands. The result of his study revealed that authority is the most popular persuasion technique irrespective of the target and the reason used. Additionally, an array of scholarly works has contended that principles of persuasion (authority, social proof, liking, distraction, reciprocation, and scarcity) are used simultaneously in social engineering related to scams (Ferreira et al., 2015; Zielinska et al., 2016; Ferreira & Teles, 2019). Scammers, pretending to be legitimate and trustworthy organizations, employ authority to influence the users. Then they also use reciprocation by offering the users something ostensibly valuable, thereby creating a sense of obligation in the victim to respond favorably. It was revealed that in over five years, reciprocation and social proof decreased while commitment/consistency and scarcity increased, demonstrating that the tactics phishers used have evolved through time. These ever-changing tactics used by fraudsters necessitate an up-to-date exploration relevant to phishing attacks.

The review of the literature reveals that phishing attacks can be approached through an exploration of their linguistic elements. Since language is used by cybercriminals in deceptive channels like phishing emails, identifying patterns, similarities, or differences between phishing and authentic emails can help educate users to detect malicious intent. Hence, this paper aimed to comparatively analyze phishing and genuine emails in terms of their language correctness and deviations, illocutionary speech acts, and persuasion principles.

3. Methodology

This study employed qualitative research, particularly textual analysis. It is a methodology used to describe, interpret, and understand language, symbols, and pictures present in texts (Caulfield, 2019). Textual analysis has been useful in this study because this work aimed to determine patterns, similarities, and differences between phishing and authentic emails.

Five (5) samples of phishing emails and also five (5) authentic emails were obtained from public posts on social media. Since this study only required samples of phishing and authentic emails, there was no need to gather the names of the individuals who posted the phishing emails on their public social media platforms, thereby protecting their identities. More so, the samples in this study included authentic bank emails from government and private financial institutions in the Philippines such as Landbank of the Philippines (LBP) and Bank of the Philippine Islands (BPI), respectively. These two banks have been mimicked by phishers to target vulnerable victims. The individuals who have received phishing emails from the impersonators of these banks have posted the actual emails on their social media platforms to warn the public to be wary of such deceptive attempts. After successfully gathering the samples, a comparative textual analysis was done to determine the patterns, similarities, and differences between phishing and authentic emails in terms of their language correctness and deviations using Murphy's (2019) English grammar reference and practice book, the illocutionary speech acts using Searle's (1969) classifications of speech acts, and the persuasion principles using Cialdini's (1984) key principles of persuasion.

4. Results and Discussions

A total of ten (10) emails comprised the data in this study. Five (5) were phishing emails (see Figure 1), and another five (5) were authentic emails (see Figure 2). A qualitative approach was then used to compare the patterns, similarities, and differences between these two sets. More specifically, the emails were examined in terms of three (3) aspects: language correctness and deviations, illocutionary acts, and persuasion principles. Figure 1 shows the first set of emails, the phishing ones.

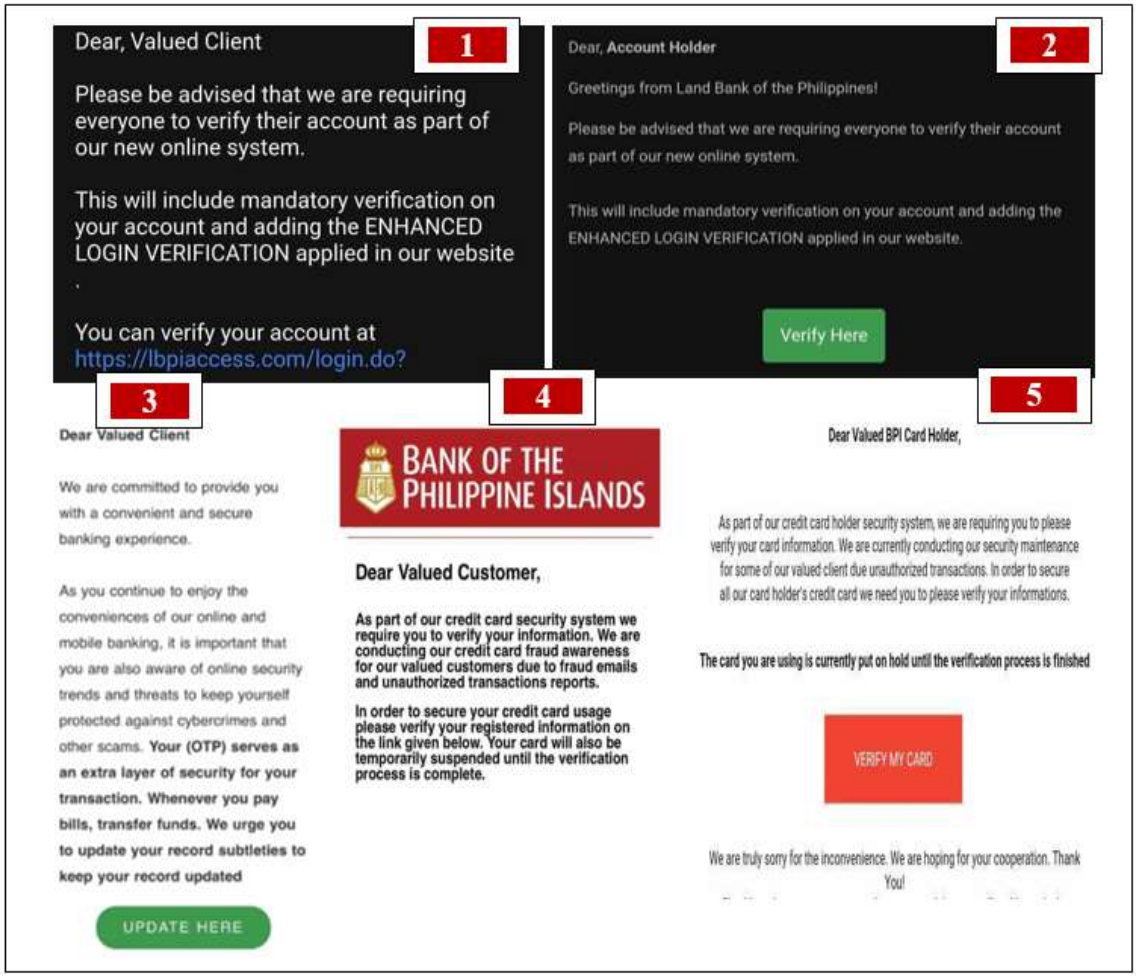

Figure 1: Phishing Emails

Figure 1 shows the five (5) phishing emails sampled in this study. Of this number, three emails were pretending to be bank emails from Land Bank of the Philippines (emails 1-3), while two (2) emails mimicked Bank of the Philippine Islands (emails 4-5). Phishing email numbers 1, 2, 4, and 5 were about verification, while the fourth one was regarding the use of OTP (One Time Pin) and a request to update the customer's bank records. The following figure below (Figure 2) shows the authentic emails.

Figure 1 shows the five (5) phishing emails sampled in this study. Of this number, three emails were pretending to be bank emails from Land Bank of the Philippines (emails 1-3), while two (2) emails mimicked Bank of the Philippine Islands (emails 4-5). Phishing email numbers 1, 2, 4, and 5 were about verification, while the fourth one was regarding the use of OTP (One Time Pin) and a request to update the customer's bank records. The following figure below (Figure 2) shows the authentic emails.

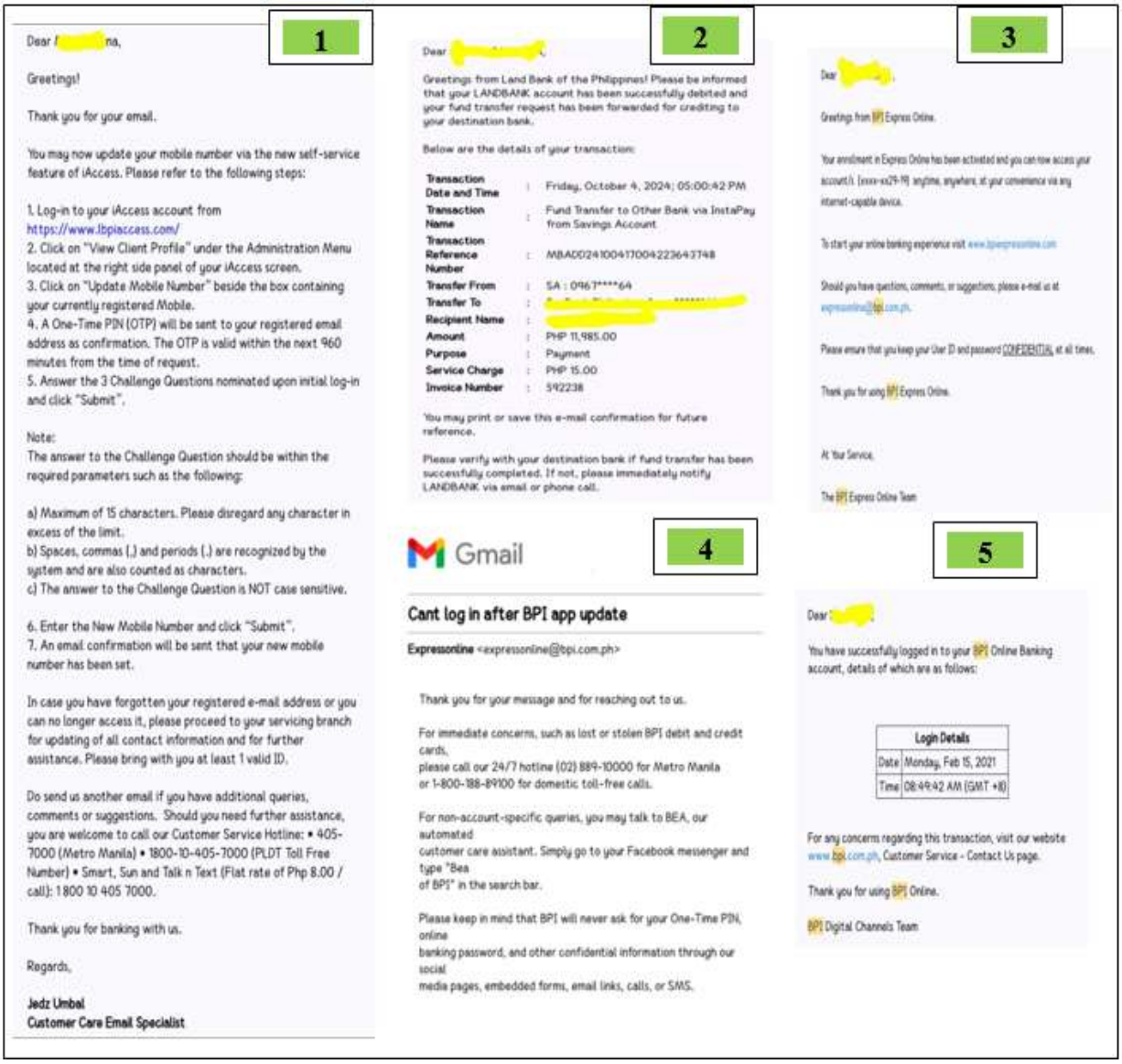

Figure 2: Authentic Emails.

Figure 2 shows the five (5) authentic emails examined in this study. Two of these emails were from Land Bank of the Philippines (emails 1-2), while three (3) were legitimate emails from Bank of the Philippine Islands (emails 4-5). Phishing email number one was regarding an update, second email was about a successful bank transfer, third was about account enrollment and activation, fourth was a response email regarding the user's inability to log in, while the fifth was an email on successful log in.

Language Correctness and Deviations in Phishing vs Authentic Emails

This section is discussed in two parts. The first part is on the language correctness between phishing and authentic emails presented in **Figure 3.a**, while the second part is on the language deviations of the same samples presented in **Figure 3.b**. Elucidations of the language correctness and deviations found in both sets of emails were anchored on Murphy's (2019) American English grammar reference and material.

Figure 3.a below presents the language correctness in phishing and authentic emails.

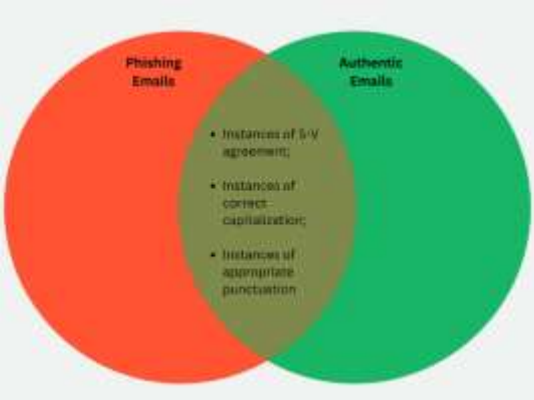

Figure 3.a: Language correctness in phishing and authentic emails.

As can be gleaned from Figure 3.a, the overlapping portion between phishing and authentic emails implies that both texts share common language correctness. Specifically, these commonalities include instances of subject-verb agreement and correct capitalization and punctuation.

The English grammar rules prescribe that the subject and verb in a sentence must agree in number. That means a singular subject takes a singular verb, while a plural subject takes a plural verb, otherwise, there will be disagreement. Instances of SV agreement were found in both phishing and authentic emails. For example, the lines ***'We are truly sorry for the inconvenience. We are hoping for your cooperation'*** from the phishing email displays proper agreement between the subject of the sentence *'we'* and the verb *'are'*. Similarly, the authentic email also follows subject-verb agreement rules such as the examples, ***'You may now update your mobile number via the new self-service feature of iAccess'*** and ***'Thank you for your message and for reaching out to us'.*** The subject 'You' in the first example agrees with the verb phrase 'may now update,' which indicates permission or ability, while the implied subject in the second example is 'We' and is understood from the context to be the Landbank of the Philippines, hence, making the sentence appropriate in a conversational setting. These excerpts are not only grammatically correct but also communicate the intended message.

Instances of correct capitalization were also visible in the sampled texts. There is a need to capitalize proper nouns ('**J**ane'), the first word of a sentence (**W**e are here), and titles (**T**o **K**ill a **M**ockingbird) except articles (a, an, the), coordinating conjunctions (and, but, or), or prepositions (in, on, at). The phishing emails display some instances of correct capitalization such as in the excerpt, '**G**reetings from **L**and **B**ank of the **P**hilippines!' 'Greetings' appears as the first word of the sentence while Land Bank of the Philippines' is the bank's proper noun, thereby necessitating them to be capitalized. The same is true with the line from the authentic email, '**G**reetings from **BPI E**xpress **O**nline. This commonality in the appropriate capitalization in phishing and authentic emails stresses the difficulty that end users may face when assessing the legitimacy of an email at face value since there are instances of correct language use in phishing emails similar to the authentic ones.

Additionally, instances of appropriate punctuation were found in both the pishing and the authentic emails. Proper punctuation such as the use of commas, periods, and other marks helps separate ideas and convey meaning. Some instances of proper punctuation were visible in both the phishing and authentic emails such as the respective examples, ***'Your OTP serves as an extra layer of security for your transaction(.)'*** and ***'Thank you for your email(.)'*** Both declarative sentences make a statement and express an opinion, thereby making the period at the end the suitable punctuation mark to use. Although these examples display proper use of punctuation in these specific contexts, there were also some instances of improper punctuation in some other parts of the sampled texts discussed in the following part and shown in Figure 3.b.

Figure 3.b capsulizes the language deviations in phishing and authentic emails.

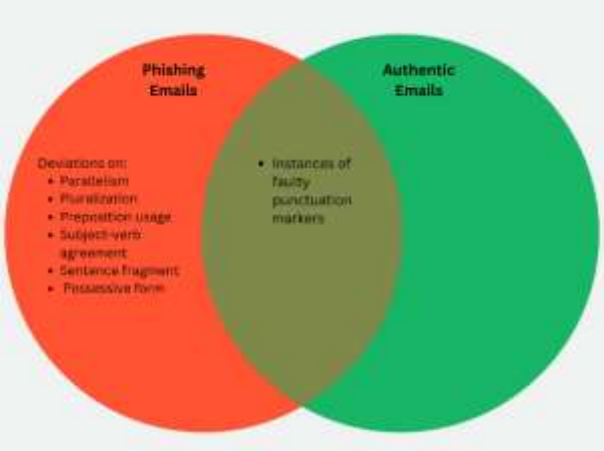

Figure 3.b: Language deviations between phishing and authentic emails.

As can be gleaned from the above figure, phishing emails display specific language deviations. Specifically, these deviations include issues with parallelism, pluralization, incorrect preposition usage, subject-verb agreement, sentence fragments, and the possessive form. These language deviations appeared exclusively in phishing emails, while both the phishing and authentic emails demonstrate some instances of faulty punctuation markers, as illustrated in the overlapping portion of the two circles.

The excerpt from the phishing email stated ***'This will include mandatory verification on your account and adding the enhanced login verification applied in our website'*** exhibits deviation on parallelism. The English grammar norm states that elements in a list or series should have the same grammatical structure to make them parallel. For example, the sentence *'She likes reading, writing, and jogging'* maintains a parallel structure, while the sentence '*She likes reading, writing, and to jog'* does not. In the phishing email's excerpt, the phrases **"*mandatory verification on your account*"** and **"*adding the enhanced login verification*"** should have been consistently structured, thereby making ***'This will include mandatory verification of your account and the addition of enhanced login verification applied on our website'*** the typical one.

Also, the line ***'We need you to please verify your informations'*** is an example of pluralization deviation found in phishing emails. In English, most nouns form the plural by adding "s" or "es." For example, "cat" becomes "cats," while "box" becomes "boxes." Certain nouns, however, like "information," "advice," and "furniture," are uncountable, therefore, they do not have a plural form. The word "information" is an uncountable noun, which means it does not have à plural form, making the cited excerpt an example of language deviation in the phishing email.

Instances of incorrect prepositions were also observed in phishing emails such as in the sentence, '***This will include mandatory verification on your account and adding the enhanced login verification applied in our website'*** where the correct prepositions should have been 'This will include mandatory verification ***(of)*** your account and the addition of enhanced login verification applied ***(on)*** our website'.

Additionally, phishing emails deviated from the prescriptive rules regarding subject and verb agreement such as in the line, ***'We are currently conducting our security maintenance for some of our valued client'.*** The absence of '**s**' after the word '**client'** is considered a deviation since it has to be pluralized to "clients" to match the quantifier 'some', meaning there are many clients involved.

Sentence fragment was also another language issue found in phishing emails. A sentence fragment is an incomplete sentence that lacks a main clause such as "*Because I was tired*". To correct it, one could say, "*I went to bed because I was tired.*" Such a fragment was found in a phishing email with the line: ***'Your OTP serves as an extra layer of security for your transaction. Whenever you pay bills, transfer funds.'*** The second part, *'Whenever you pay bills, transfer funds',* was a fragment and should have been combined with the previous sentence for clarity, thus making the correct sentence, 'Your OTP serves as an extra layer of security for your transaction whenever you pay bills and transfer funds.'

Finally, an incorrect possessive form was also found in phishing emails such as the line, ***'In order to secure all our card holder's credit card, we need you to please verify your information.'*** To form the possessive of plural nouns that end in "s," an apostrophe has to be added after the "s." For example, "*the dogs' owner*" indicates that multiple dogs belong to the same owner. The possessive form ***'cardholder's'*** in the phishing email, however, displays a faulty possessive form since the ***'card holder's'*** needs to be changed to the plural possessive, correcting it into, ***'In order to secure all our cardholders' credit cards, we need you to please verify your information.'***

The overlapping portion of Figure 3.b above also shows the commonality between phishing and authentic emails and that is the instances of faulty punctuation markers. These instances were shown through a misplaced comma, à lack of à comma, and à lack of a period in the parts where these punctuations were deemed necessary. Examples of these are lines from phishing emails**, *'Dear, Valued Client',*** and ***'As part of our credit card security system we require you to verify your information.'*** The first example displays a misplacement of the comma where it appeared after the word *'Dear'* instead of the whole salutation *'Dear Valued Client (,)'*. Also, the second example lacks a comma after the subordinate clause. The correct sentence should have been ***'As part of our credit card security system, we require you to verify your information.'*** Adding the comma clarifies that the introductory clause is separate from the main idea of the sentence, thereby enhancing overall comprehension. Another sentence from the phishing email lacks proper punctuation such as in the line, ***'The card you are using is currently put on hold until the verification process is finished*** (no period)**'.** A period should have been placed after the word ***'finished'*** as it conveys a complete thought.

Interestingly, these punctuation inaccuracies are not exclusive to phishing emails. Even authentic emails commit punctuation inaccuracies such as in the excerpt from an authentic LBP email: ***'Please be informed that your Landbank account has been successfully debited and your fund transfer request has been forwarded for crediting to your destination bank.'*** This compound sentence combines two independent clauses**(1) *Please be informed that your Landbank account has been successfully debited'*** and (2) *'**your fund transfer request has been forwarded for crediting to your destination bank'*** joined by the coordination conjunction ***'and'.*** The prescriptive rule says a comma should be placed before the coordinating conjunction when it connects two independent clauses. In this case, a comma needed to be placed before the word 'and'. The same issue has been found in a legitimate BPI email such as the line: ***'Your enrollment in Express Online has been activated and you can now access your account anytime.'*** This compound sentence also consists of two independent clauses connected by the coordinating conjunction ***'and'*** but without the necessary comma.

These results reveal that although phishing emails commit more linguistic deviations than authentic emails, the latter is also not free from all types of blemishes, thereby making it difficult to distinguish the fake from the legitimate when paying attention only to linguistic deviations as separating cues. This finding coincides with the previous works indicating that language correctness cannot be used as a reliable means to detect phishing attempts (Blythe et al., 2011; Peng et al., 2018). Since instances of language incorrectness are present in both phishing and genuine bank emails, solely relying on grammatical cues may not be sufficient to detect a scam especially since the clarity of the message is maintained in phishing emails despite the deviations.

Illocutionary Acts in Phishing vs Authentic Emails

The second linguistic aspect considered in the comparison of phishing and authentic emails in this study is the illocutionary act. Figure 4 presents the illocutionary acts found in phishing and authentic emails.

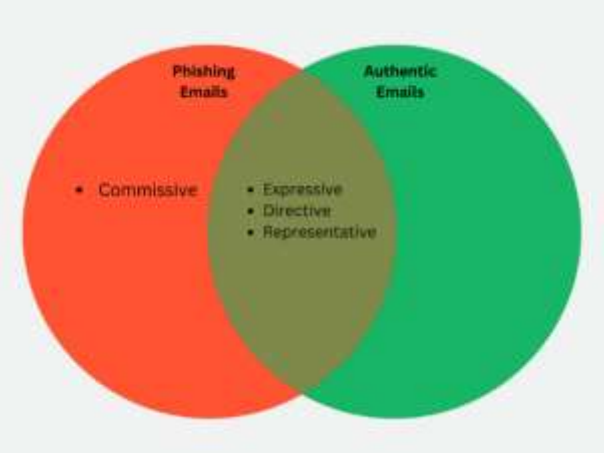

Figure 4: Illocutionary speech acts in phishing and authentic emails.

As the figure presents, three illocutionary speech acts were present in both phishing and authentic emails: expressive, directive, and representative acts. The expressive acts were used to foster goodwill and strengthen social bonds in the communicative environment. In the phishing emails, the use of the sentence, ***'We are truly sorry for the inconvenience…*** and the line, ***'Thank you for your message and for reaching out to us…'*** in the authentic emails not only express apology and thanks but also acknowledges that the relationship they have with their clients is paid a high value. Based on the account of Searle's (1969) categorization of illocutionary acts, appreciating, apologizing, thanking, and greeting are categorized as expressive. This kind of illocutionary act are utterances that are articulated to express the speaker's feelings and emotions about themselves and even the

world around them. The use of the expressive act in the context of phishing emails is no different from the way it is used in authentic bank emails. Both legit and scam emails establish communicative environments that give support to the users by acknowledging their feelings which in turn can provide comfort and validation.

The directive and the commissive acts were also visible in both phishing and authentic emails. These two acts appear in a single email at the same time. For instance, in the phishing email: ***'As part of our credit card security system, we require you to verify your information'*** (commanding). ***We are conducting our credit card fraud awareness for our valued customers due to fraud emails and unauthorized transactions reports'*** (stating/describing), the phisher commands the target to verify his/her bank details and then proceeds to inform the same target that there is an ongoing credit card awareness campaign after the alleged reports of unauthorized transactions. In the authentic emails, both of these acts were also observed such as in the lines, '***Please be informed that your Landbank account has been successfully debited and your fund transfer request has been forwarded for crediting to your destination bank'*** (stating/describing); ***Please verify with your destination bank if the fund transfer has been successfully completed'*** (directive). In this excerpt, the user received a legitimate email from LBP informing him/her that the recent bank transfer he/she made was successful, and then the same person was instructed to check if the amount had indeed reached the destination bank. In both the phishing and authentic emails, the blend of informing and requesting can be observed. Taking into account Searle's (1969) categorization of the illocutionary act, requesting or commanding is under the directive act while informing is under the representative. This result implies that the representative and the directive acts are inseparable in either phishing or authentic emails because these two acts are fundamental in conveying information and facilitating action.

Interestingly, instances of the use of commissive acts were found in the phishing emails. According to Searle's (1969) categorization of illocutionary acts, commissive acts include promising, offering, vowing, threatening, warning, betting, and challenging. The commissive act is a type of illocutionary act where the speaker commits to doing a certain course of action, whether it be positive like promises, or negative like threats. In the case of the sampled phishing emails, the commissive acts were found in the facade of the representative act such as in the lines: ***'Your card will be temporarily suspended until the verification process is complete'*** and ***'The card you are using is currently put on hold until the verification process is finished.'*** Examining these sentences at the surface level may tell that these lines merely inform, describe, or state details such that the user's card is placed on hold. While this may be true, one may also argue that the implied consequence of these sentences conveys a threatening undertone that if the user will not do the required verification, then a course of action may be taken and that is suspending his/her account.

This result reveals that a threat may be presented in other subtle forms like informing or stating, all while maintaining the communicative force of such a threat. This study further shows that phishing and authentic bank emails differ in this manner. While authentic bank emails avoid threatening language like citing that the user's account may have to be suspended or put on hold, phishing emails use commissive acts to influence and facilitate actions or responses from the end users. These findings coincide with the previous studies of Chiluwa (2010) which found that phishing emails employ speech acts such as expressive, representative, commissive, and directive acts, and also that of Brooks (2018) which revealed that threats (commissive) are among the common acts used in phishing emails, and the works of Carvalho (2011), Malka et al. (2015), and Unnam et al. (2019) which cite that authentic professional emails often involves speech acts like requests but maintains a respectful tone throughout the message.

Persuasion Principles in Phishing vs Authentic Emails

The third aspect considered in comparing the phishing and authentic emails in this study is the use of persuasion principles. Thus, figure 5 shows the principles of persuasion reflected in phishing and authentic emails.

Figure 5: Persuasion principles in phishing and authentic emails.

As the figure presents, one persuasion principle is common between phishing and authentic emails, and that is the use of authority. According to Cialdini (1984), people often tend to believe individuals who appear credible. It may be expected for phishing emails to use authority since phishers pretend to be legitimate institutions. The use of authority as a persuasion principle in both phishing and authentic emails is exhibited in the following excerpts: ***'Greetings from Landbank of the Philippines!'; 'Greetings from BPI Express Online.'*** These brief pleasantries not only serve to address the email recipient and set a friendly tone for the communication right at the beginning but also establish authority and identity. These greetings help inform the recipients that the instructions they are about to read in the emails are from their financial institutions, only that in phishing emails, they are but imposters.

Apart from greetings, authority can also be observed in the emails' use of authoritative tone and business jargons. Such is depicted in the following excerpts from phishing emails: ***'This will include mandatory verification on your account and adding the enhanced log-in verification applied in our website'***, and '***Your OTP serves as an extra layer of security for your transaction'***. These excerpts display straightforward and authoritative tone, just as the ones used in the authentic emails like: ***'You may now update your mobile number via the new self-service feature of iAccess…'*** This commonality in the use of authority between the real emails and the reeling ones implies that end users may face difficulty distinguishing fake from the authentic considering that phishers have also adopted similar tones and jargon in their emails. Nevertheless, one thing observable in the phishing emails is the repetitive use of the words ***'mandatory', 'suspended',*** and ***'on hold'*** which may have been used deliberately to encourage the victims to act promptly. This means that phishers hide behind the facade of their fake authority to evoke a sense of urgency.

Notably, this study found out that apart from authority, the principles of reciprocity, social proof, and liking were the other persuasion principles employed in phishing emails and not in authentic emails. Cialdini's (1984) principle of reciprocity describes that people are more likely to accept a request out of feeling that they owe the person something. An example of how this is used in phishing emails is the excerpt, ***'We are truly sorry for the inconvenience. We are hoping for your cooperation.'*** By stating these, the speaker is implying that they have already made efforts for the benefit of the end users, thereby creating a sense of obligation upon him/her to reciprocate the goodwill.

Social proof, on the other hand, talks about how people often trust something if they see some other people who have tried exactly the same thing or who were in the same situation. This is exhibited in the phishing email's use of the line, ***'Please be advised that we are requiring everyone to verify their account as part of our new online system.'*** The inclusion of the word 'everyone' in this sentence was done deliberately to convey that the recipient is not the only one compelled to do the verification. Others were also required, and since he/she was not the only one, the verification must have been necessary and legitimate.

Finally, liking means people are more likely to believe those they like rather than those they do not appreciate. This principle is depicted in the phishing email's use of '***Dear Valued Client', 'Dear Valued BPI Card Holder',*** or ***'Dear Valued Customer'.*** While authentic emails make use of specific and personal salutations like, ***'Dear Mr. Abra',*** or ***'Dear Ms. Angela Santos',*** phishing emails are a generic copy sent to as many people as possible, thus salutations are not personalized and instead use the term, 'valued'. Referring to someone as a *'valued customer'* may convey appreciation and respect such as in the case of phishing emails. The deliberate use of the salutation *'Dear Valued Client'* is a means to make the recipient feel more regarded and liked, thereby increasing the likelihood of these recipients taking the bait. The result of this study is cognizant of the previous works indicating that the success of phishing attacks depends on the effective exploitation of human weakness, specifically citing that authority is mostly present in phishing emails along with the simultaneous use of the other persuasion principles (Akbar, 2014; Ferreira et al., 2015; Zielinska et al., 2016; Rajivan & Gonzales, 2018; Ferreira & Teles, 2019).

Drawing the Line between the Genuine and the Copycat

Three crucial findings shape the inferences of this study in outlining the linguistic cues that set apart a fake email from genuine ones. Firstly, this work reveals that although there are more linguistic deviations in phishing emails, there are also instances of language correctness in the same text samples. Similarly, although more language correctness was displayed in authentic emails, these emails were not 100% error-free as there were observed instances of deviations in the authentic emails too. These results imply that focusing on the grammatical cues may not fully unmask the imposters since both fake and legitimate emails share common correctness and deviations. Secondly, this paper reveals that, unlike legit emails that avoid threatening language such as citing that the user's account may have to be suspended or put on hold, phishers convey messages that appear like simple informing and stating at face value but are subtle threats. This means that unlike the legitimate, the copycat hides their true agenda behind innocent statements and descriptions. Thirdly, this work reveals that authority was typical in both phishing and authentic emails, but phishing employs other persuasion principles by making the recipients feel like they owe them something, by citing social proof, and by building à connection. This suggests that the copycat's scheme may include stimulating people's emotions, thereby driving them to take action.

The findings of this work support existing studies that have previously underscored the influential role language plays in manipulation and deception (Brooks, 2018; Chen, 2021; Hazra & Majumder, 2024). Posing as legitimate entities, phishers aim to be as persuasive as possible in their emails by establishing a sense of urgency or authority. This, however, serves as the Waterloo in their tactics. Since genuine emails from legitimate institutions maintain authority without necessarily casting a sense of urgency or subtle threats upon their clientele, detecting such use of threats in phishing emails is one way to draw the line between the original and the copycat. To put it simply, what sets apart a fake from a genuine one is not merely the linguistic quality of the text but the communicative intentions hiding behind the facade of the email's linguistic value. Considering these results, it can be deduced that avoiding a scam entails one to detect hidden schemes conveyed through the email's language.

5. Conclusion

In conclusion, this study aimed to understand how phishing and authentic emails converge or diverge in terms of their language correctness and deviations, illocutionary speech acts, and principles of persuasion. These aspects were given focus considering that language plays an important role in any human activity including manipulation and deception. The comparative analysis consists of identifying how the language of fake emails emulates or deviates from the norms present in genuine emails, thereby allowing the researcher to pinpoint possible red flags that may unmask the pretending scammers.

Three important findings of this research are: First, although phishing emails commit more types of deviations than authentic emails, authentic ones also display a few instances of grammatical inconsistencies, thereby making it unreliable to set apart a copycat from the genuine when focusing solely on their language correctness or deviations. Second, while both the phishing and the authentic emails employ expressive, directive, and representative acts, the commissive act appears exclusive to phishing through subtle threats, indicating that a threatening email may be a reeling email leading the victims to take the bait. Lastly, the display of authority was typical in both phishing and authentic emails, but the former employs other persuasion principles such as reciprocity, social proof, and liking, suggesting that phishers aim to increase their chance to succeed by not only impersonating legitimate institutions but by also stimulating the victims' emotions. Based on these findings, this study concludes that what draws the line between real emails and reeling ones is not mainly language correctness or deviations since phishers could replicate the language structure of the authentic text. Rather, it is the phishing email's tendency to evoke feelings of fear and a sense of urgency behind their language that may give their deception away.

6. Study Limitations and Future Research

Although this work may be useful in distinguishing linguistic elements separating the genuine from the fake, one limitation of this study, however, is that the phishing emails sampled in this work speak only of the tactics that phishers employ in the present. Since their strategies may continue to evolve through time, more relevant works in the years to come may reveal new insights into the problem this work aimed to address. Thus, up-to-date research on this area may be necessary. Despite this limitation, nevertheless, the findings of this present work may help inform users of the ways to detect emails that are real and emails that try to reel them into the phishing trap.

Funding: This research received no external funding.
Conflicts of Interest: The author declare no conflict of interest.
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] Aggarwal, S., Kumar, V., & Sudarsan, S. D. (2014, September). Identification and detection of phishing emails using natural language processing techniques. In Proceedings of the 7th International Conference on Security of Information and Networks (pp. 217-222).

[2] Akbar, N. (2014). Analysing persuasion principles in phishing emails. Master thesis. University of Twente. Enschede, Netherlands

[3] Aksu, D., Abdulwakil, A., & Aydin, M. A. (2017). Detecting phishing websites using support vector machine algorithm. PressAcademia Procedia, 5(1), 139-142.

[4] Alam, M. N., Sarma, D., Lima, F. F., Saha, I., & Hossain, S. (2020, August). Phishing attacks detection using machine learning approach. In 2020 third international conference on smart systems and inventive technology (ICSSIT) (pp. 1173-1179). IEEE.

[5] Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science, 3, 563060.

[6] Arévalo, D., Valarezo, D., Fuertes, W., Cazares, M. F., Andrade, R. O., & Macas, M. (2023, July). Human and Cognitive Factors involved in Phishing Detection. A Literature Review. In 2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE) (pp. 608-614). IEEE.

[7] Asani, E., Omotosho, A., Danquah, P., Ayoola, J., Ayegba, P. & Longe, O. (2021). A maximum entropy classification scheme for phishing detection using parsimonious features. Telkomnika Telecommunication, Computing, Electronics and Control. Vol. 19, No. 5, October 2021, pp. 1707~1714

[8] Austin, J. L. (1962). How to do things with words. Oxford: University Press.

[9] Baykara, M. & Gürel, Z. Z. (2018). Detection of phishing attacks. 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 2018, pp. 1-5, doi:10.1109/ISDFS.2018.8355389.

[10] Blythe, M., Petrie, H., & Clark, J. A. (2011, May). F for fake: four studies on how we fall for phish. In Proceedings of the SIGCHI conference on human factors in computing systems (pp. 3469-3478).

[11] Brooks, H. S. (2018). Linguistic persuasion techniques in phishing emails: A corpus and critical discourse analysis. Hofstra University.

[12] Budiharto, R. A. (2016, January). Language deviations in a popular novel: An alternative way to teach morphology and phonology for English Department Students of Madura University. In Proceeding of International Conference on Teacher Training and Education (Vol. 1, No. 1).

[13] Cardona, J. (2024). Grammatical Deviations in Philippine Phishing Emails. International Journal of English Language Studies, 6(2), 124-129.

[14] Carvalho, V. R. (2011). Email "Speech Acts". Modeling Intention in Email: Speech Acts, Information Leaks and Recommendation Models, 5-34.

[15] Carvalho, V. R., & Cohen, W. W. (2005, August). On the collective classification of email" speech acts". In Proceedings of the 28th annual international ACM SIGIR conference on Research and development in information retrieval (pp. 345-352).

[16] Caulfield, J. (2019). Textual analysis. Guide, 3 approaches & examples. Scribbr. https://www.scribbr.com/methodology/textual-analysis/

[17] Chandrasekaran, M., Narayanan, K. & Upadhyaya, S. (2006). Phishing e-mail detection based on structural properties. NYS cyber security conference (Vol. 3, pp. 2-8).

[18] Chen, J. (2021). "You are in trouble!": A discursive psychological analysis of threatening language in Chinese cellphone fraud interactions. International Journal for the Semiotics of Law-Revue internationale de Sémiotique juridique, 34, 1065-1092.

[19] Chen, T. C., Stepan, T., Dick, S., & Miller, J. (2014). An anti-phishing system employing diffused information. ACM Transactions on Information and System Security (TISSEC), 16(4), 1-31.

[20] Chiluwa, I. (2010). The pragmatics of hoax email business proposals. Linguistik online, 43(3), 3-17.

[21] Chowdhary, S. K., Kumar, P., Mittal, R., Gumber, I., Jangra, V., & Srivastava, P. (2024). Phishing detection tool for financial emails. International Journal of Financial Engineering, 2442002.

[22] Cialdini, R. B. (1984). Influence: The psychology of persuasion. William Morrow.

[23] Ferreira, A., & Teles, S. (2019). Persuasion: How phishing emails can influence users and bypass security measures. International Journal of Human-Computer Studies, 125, 19-31.

[24] Ferreira, A., Coventry, L., & Lenzini, G. (2015). Principles of persuasion in social engineering and their use in phishing. In Human Aspects of Information Security, Privacy, and Trust: Third International Conference, HAS 2015, Held as Part of HCI International 2015, Los Angeles, CA, USA, August 2-7, 2015. Proceedings 3 (pp. 36-47). Springer International Publishing.

[25] Hani, Aineena. (2021, July 14). Dealing with the rise in phishing attacks in the Philippines. Retrieved from https://opengovasia.com/dealing-with-the-rise-in-phishing-attacks-in-the-philippines/

[26] Hazra, S., & Majumder, B. P. (2024, June). To tell the truth: Language of deception and language models. In Proceedings of the 2024 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies (Volume 1: Long Papers) (pp. 8498-8512).

[27] Kim, S. H., Jim, S. H., Cho, J. M., Cho, Y. S., Cho, S. R., Noh, J. H., & Choi, D. S. (2014). U.S. Patent Application No. 13/946,803.

[28] Kumar, S., & Gouda, S. (2023). A comprehensive study of phishing attacks and their countermeasures. International Journal of Research and Analytical Reviews, 10, 25-31.

[29] Larsen-Freeman, D. (2003). Teaching and principles in language teaching. Oxford University Press.

[30] Malka, S. T., Kessler, C. S., Abraham, J., Emmet, T. W., & Wilbur, L. (2015). Professional e-mail communication among health care providers: proposing evidence-based guidelines. Academic Medicine, 90(1), 25-29.

[31] Murphy, R. (2019). English grammar in use: A self-study reference and practice book for intermediate learners of English (5th ed.). Cambridge University Press.

[32] Park, G., Stuart, L.M., Taylor, G.M. & Raskin, V. (2014). Comparing machine and human ability to detect phishing emails. IEEE International Conference on Systems, Man, and Cybernetics (SMC), San Diego, CA, USA, pp. 2322-2327, doi: 10.1109/SMC.2014.6974273.

[33] Park, G., Stuart, L.M., Taylor, G.M. & Raskin, V. (2014). Comparing machine and human ability to detect phishing emails. IEEE International Conference on Systems, Man, and Cybernetics (SMC), San Diego, CA, USA, pp. 2322-2327, doi: 10.1109/SMC.2014.6974273.

[34] Patel, H., Rehman, U., & Iqbal, F. (2024). Large language models spot phishing emails with surprising accuracy: A comparative analysis of performance. arXiv preprint arXiv:2404.15485.

[35] Peng, T., Harris, I., & Sawa, Y. (2018, January). Detecting phishing attacks using natural language processing and machine learning. In 2018 ieee 12th international conference on semantic computing (icsc) (pp. 300-301). IEEE.
[36] Pietrantonio, F., Botta, A., Zinno, S., Ventre, G., Gallo, L., Mancuso, L., & Presta, R. (2024, June). A Gaze-Based Analysis of Human Detection of Email Phishing. In 2024 Silicon Valley Cybersecurity Conference (SVCC) (pp. 1-8). IEEE.
[37] Priya, S., Gutema, D., & Singh, S. (2024, March). A Comprehensive Survey of Recent Phishing Attacks Detection Techniques. In 2024 5th International Conference on Innovative Trends in Information Technology (ICITIIT) (pp. 1-6). IEEE.
[38] Proudfoot, J.G., Giboney, J. S., Schuetzler, R. & Durcikova, R. (2011). Trends in phishing attacks: suggestions for future research. Research in progress. Information Systems and Quantitative Analysis Faculty Proceedings & Presentations.
[39] Rajivan, P., & Gonzalez, C. (2018). Creative persuasion: a study on adversarial behaviors and strategies in phishing attacks. Frontiers in Psychology, 9, 135.
[40] Rawat, S., & Kunwar, H. (2023, August). An Integrated Review Study on Efficient Methods for Protecting Users from Phishing Attacks. In 2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS) (pp. 1286-1289). IEEE.
[41] Searle, John R. (1969): Speech Acts. Cambridge.
[42] Singer, P. W., & Friedman, A. (2014). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.
[43] Statista. (2022, December 15). Number of phishing attacks in the Philippines in 2021 to 1st half of 2022. Retrieved from https://www.statista.com/statistics/1349352/philippines-number-of-phishing-attacks/
[44] Swan, M. (2005). Practical English usage (3rd ed.). Oxford University Press.
[45] Unnam, A., Takhar, R., & Aggarwal, V. (2019). Grading Emails and Generating Feedback. International Educational Data Mining Society.
[46] Yaghubyan, M. (2020). Linguistic Deviation in Business Advertisements. Armenian Folia Anglistika, 16(2 (22)), 9-19.
[47] Zielinska, O., Welk, A., Mayhorn, C. B., & Murphy-Hill, E. (2016, April). The persuasive phish: Examining the social psychological principles hidden in phishing emails. In Proceedings of the Symposium and Bootcamp on the Science of Security (pp. 126-126).