International Journal of Research and Review
Volume 11; Issue: 7; July 2024
Website: www.ijrrjournal.com
Short Communication *E-ISSN: 2349-9788; P-ISSN: 2454-2237*

Bank Emails: The Language of Legit and Scam

Sophomore T. Vacalares[1], Brian Paul E. Sta. Ana[2], Daryl Q. Dranto[3], Jinky S. Gallano[4]

[1,3,4]Opol Community College, College of Education, Opol, Misamis Oriental, Philippines
[2]Pilar National High School, Surigao del Norte, Philippines

Corresponding Author: Sophomore Talle Vacalares

DOI: https://doi.org/10.52403/ijrr.20240721

ABSTRACT

Amidst the pandemic, the surge in unsolicited scam emails has made internet technology a significant concern. Distinguishing between scams and authentic/ legit emails has become increasingly difficult. This research aimed to identify typical characteristics and language patterns found in emails. It also aimed to identify the common linguistics and technical features of the scams and legitimate bank emails. Two legitimate emails and two scam or fraudulent emails from different banks in the Philippines (i.e., LandBank and BDO). A qualitative method was used to analyze and interpret the language features of the two emails. This led to the identification of shared characteristics found in scams and legitimate emails. A scam email typically includes embedded malicious links, misspellings, formatting issues, suspicious email domains, frequent use of contractions and redundancy, tautology, and imperative mood. On the other hand, legitimate emails exhibit proper punctuation, accurate email domains, appropriate formatting, absence of spelling mistakes, avoidance of contractions and redundancy, and use indicative mood rather than imperative. Scam emails utilize modal verbs to manipulate recipients into divulging personal information. Recognizing these email patterns is crucial for educating users and reducing phishing risks. It is important to note that the interpretation and findings of this study are based on the entire dataset collected.

Keywords: Bank Emails, Legit Emails, Linguistic Features, Scam Emails, Phishing

INTRODUCTION

Emails have emerged as one of the most straightforward and rapid communication methods used by individuals. Their utilization has surged over numerous years. Due to its reputation as a cost-effective and swift communication tool, individuals find it easy to exchange personal and professional information or place orders via email (Ali Taha et al., 2021). Today, business is conducted online because of the expansion of internet usage to the time of the incident of the pandemic (Lugtu, 2021). Submitting online payment details such as bank transfers, GCash, and credit card information creates more opportunities for thieves to fraudulently obtain personal data, including passwords and credit card details. As internet usage continues to rise, individuals find greater ease in divulging their information online and exchanging data with others via the internet rather than through manual methods (Ali Taha et al., 2021). Cybercriminals can execute financial scams due to the substantial number of transactions taking place via websites, the Internet, and email.

Utilizing technology without a structured approach is merely a time-wasting endeavor (Crismundo, 2021). Employing technology

necessitates appropriate methods to ensure it yields optimal benefits for users. This also applies to emails, which undoubtedly offer convenience to individuals, yet numerous aspects require individual attention and action (to be addressed by users themselves). With the emergence of digital fraud, there is frequent confusion between scams and spam. Spam refers to unsolicited emails sent in large quantities without consideration for their content. In the same regard, another view of spam is a broad classification of all types of undesirable and unsolicited internet messaging. This work states that online is normally associated with e-mail, spam distribution, and spamming; nevertheless, online existed before the normalization of e-mail (Allen, 2017).

Phishing can be described as an attempt by an unscrupulous person to obtain, for personal gain, information such as usernames, passwords, and credit card details by feigning credibility in a computer-based communication. Winning notices that resemble widespread social networks, apps for purchases, online payment services, or IT supervisors are typically used to mislead people. These phishing emails might contain web links that take the users to other sites that have been planted with other malicious codes or programs (Bhavsar et al., 2018). Phishing has been a long-standing tactic used by attackers, and organizations are actively engaged in countering it through detection tools, informational campaigns, and user education. However, despite all these efforts, phishing attacks continue to occur and are still effective with losses running to millions of US dollars.

At times the scam emails and the legitimate ones may not be very easy for anyone to differentiate and this may be very complicated to some of the smart fraudsters who are willing to go the extra mile in the latest technological developments (Datar et al., 2014). The main objective of this study therefore is to examine the language or linguistic level used by the end users of emails in cyber fraud. However, with the emerging advanced email heist, it becomes difficult to differentiate the given emails from the valid ones. According to the National Bureau of Investigation, typical scam emails may feature an awkward greeting; misspelling and/or grammatical mistakes; multiple email addresses, links, and/or domain names, especially if contrasting; a pressing tone; suspicious, large or unknown attachments; short and peculiar requests, as well as requests for personal information and/or payment information.

Scammers often target organizations that are popular and with a good reputation, including banks, shopping centers, government offices, and schools, to trick people and obtain private details. But it often becomes difficult to differentiate these desperate attempts as the email looks like it came from a genuine source, for example, the BDO Company which often sends email statements to its clients. In such scenarios, scammers may send fraudulent emails requesting changes to usernames and passwords or soliciting sensitive information like card numbers and PINs. This leads individuals to unwittingly disclose this information, assuming it is a legitimate request. Understanding how users discern between scam and authentic emails holds significant importance. This study aims to comprehensively outline the common traits and cues that users can utilize when differentiating between scam and legitimate emails.

MATERIALS & METHODS

A qualitative method was used to interpret and identify the significant linguistic features of the scam and legitimate emails. Textual analysis encompasses a methodical examination and interpretation of written, spoken, or visual content aimed at revealing patterns, meanings, and linguistic features present within the two emails.

The email sample was extracted from public posts on social media, thereby eliminating the need for the researcher's email account consent. The data sample comprised a blend of various established private banks and government agencies. The researcher

meticulously examined the specifics and emphasized essential cues, such as employing renowned company names, replicating email addresses, verifying bank links or URLs, aligning with the format of authentic emails, and assessing the language utilized.

Finally, a comparative analysis was utilized to distinguish unique language patterns and shared characteristics or cues between legitimate and fraudulent emails originating from a well-known bank, in addition to the distinct markers and linguistic features of the two types of emails. Among the two emails assessed, one was an instance of a personal information scam reported by a social media user on Facebook. Meanwhile, the other emails (refer to Fig. 2) were authentic or legitimate correspondences from the bank. Specifically, Figure 1 comprised a fraudulent or scammer attempt to deactivate a bank account and a deceptive request for verification.

RESULTS & DISCUSSION

Qualitative approaches were employed in this study to pinpoint the significant distinguishing features of both scam and authentic emails. In the discussion section, the study highlights the application of qualitative methods in scrutinizing and contrasting the language utilized in scam and legitimate emails.

1. Linguistic Features of Scam Emails

Social engineering, involving the manipulation of individuals, has emerged as a highly damaging method used in computer system attacks. Attackers exploit human vulnerabilities to bypass technical security measures to obtain login details, social security numbers, credit card data, or even system access (Salahdine & Kaabouch, 2019). For attackers, humans represent the most accessible gateway into a network, contributing to 95% of security incidents in corporate environments (Diaz et al., 2020).

1.2. Faulty Punctuation Markers: Comma

Fraudsters might employ misleading addresses, authentic-seeming logos, and fake web links within these emails. Within this sample email, there were noticeable indicators of phishing and scam elements that require careful observation. First, email 1 was one of the common and classic scams since it was written by individuals who could barely write proper English but were attempting to use language to persuade, deceive, calm, and/or emotionally appeal to the readers. Fraudsters commonly exploit reputable companies to phish personal and banking details from clients. This email was identified as a scam because of prevalent typographical mistakes in the text. Specifically, it was noted that in the email's greeting, the scammer omitted appropriate punctuation, such as a comma or colon at the end (for instance, "Dear Valued Client"). As with Schaffer's (2012) study, he also discovered that fake messages had other punctuation flaws (ranging from missing or misplaced apostrophes to incorrect usage of periods, quotation marks, and colons).

1.3. Non-personalize Salutations

In a letter or an e-mail, the greeting or greeting line acts as the opening, where the writer introduces him- or herself to the addressee. Greetings, farewells, and other elements of the message's closings depicted its politeness and social distance (Kim et al ., 2016). Typically, the salutation starts with the appearance of the word Dear followed by the <person's name or title> followed by a comma or a colon (Bommaert & Omoniyi, 2006) (for example, Dear Mr. Dela Cruz,). This corresponds to the following correspondence form which is much more personal (see Fig. 2) than the following fraudulent email which is too generic (see Fig. 1). In fact, several studies have reported an increase in response rate when the greeting is 'Dear', <person's name> rather than 'Dear Sir/Madam' (Brennan, 1992). Secondly, personalization suggested by Dillman (2000), based on the social exchange theory, is important and attention because they were made to feel special.

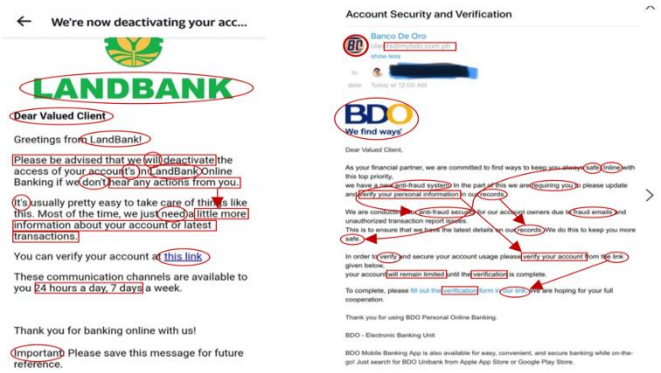


Figure 1. Scam or Fraudulent Email

1.4. Tautology

Tautology refers to the redundant or repetition of words, expressing the same concept repeatedly in varying terms. It serves the purpose of either restating an identical message or emphasizing an idea that was recently conveyed (Pomorska, 1987; Al-Marsumi, 2017). In this case, fraudulent emails (see LandBank scam email) contain repetition of the bank name to persuade and convince the clients that the email is coming from the official bank statement. Also, the sentence 'if we don't hear any actions from you' is reiterated differently by adding information 'we just need a little more information about your account or latest transactions' to convince the client to disclose information. This is supported by the study of Hassan & Barber (2021), which shows that repeated exposure to information can influence beliefs regarding its truthfulness. When individuals encounter claims multiple times, they tend to perceive them as more valid. This phenomenon, known as the illusory truth effect (Altalhab, 2018), sheds light on why advertising, propaganda, and the acceptance of fake news occur.

Moreover, the same thing happened in the BDO scam email, the repeated words 'anti-fraud,' 'verify,' 'safe,' 'verification,' and 'records.' When information is repeated, it becomes easier to understand and, therefore, seems more truthful. This idea, supported by studies like Unkelbach (2007) and Unkelbach & Stahl (2009), suggests that our brains link ease of understanding (fluency) with truthfulness. This connection happens because, over time, we have learned that when something is easy to process, it often appears more truthful, even though the truth itself is not always readily observable (Unkelbach & Greifeneder 2013).

1.5. Orthographic and Indentation Errors

Phishers often craft emails that closely resemble genuine ones, aiming to deceive users into opening an attachment or clicking on a link. Some of these deceptive emails manage to bypass spam filters due to the deliberate inclusion of misspelled words (Alkhalil et al., 2021). Orthographical errors, particularly evident in the initial sentence, are noticeable in the term "Inline." The absence of a space between "In" and "line" alters the intended meaning. Merriam's Dictionary distinguishes the word "Inline" (an adjective) as having parts arranged in a line, while "In line" (a prepositional phrase) signifies being in agreement.

Similarly, the second line appears to be missing a comma after the introductory phase "In the part of this" and after the word "usage" which belongs to the introductory clause of the given sentence. Furthermore, in that same line used, there is a concern about the progressive of the verb 'requiring.' It may a mistake when, in its place, should be used a simple tense, 'require'. Similarly, in the fourth line, the scammer employed the compound adjective "safe" rather than the comparative form "safer," resulting in a less clear and wordier construction. As a result,

methods that identify fraudulent emails by scrutinizing spelling and grammar are gaining prominence. These approaches aim to prevent such emails from reaching the user's inbox (Alkhalil et al., 2021).

1.6. Apostrophes and Contractions

The contemporary English apostrophe serves two main purposes: indicating omitted letters or denoting the genitive case in singular or plural forms. Conversely, the genitive apostrophe functions as a marker for either indicating possession or representing close association (Lasota, 2008). It was seen that the correct usage of apostrophe (‘s) was missing while using the word account. An apostrophe (’s) may be used in contractions of words like from the word ‘is’ or ‘us’ as well as possessive if one personally wants to portray that something belongs to something or someone (Collins et al., 1997). The icon ‘s’ employed in the word ‘account’ inside the email is not appropriate as a contraction or possessive, making it otherwise grammatically wrong. To illustrate this, Insley (2016) categorized formal texts which include bank emails or business letters, with the belief that they convey information; direct strategy, indirect strategy, and persuasive strategy. Writing a formal email implies considerable attention to small things and no mistakes. Writing a business or a formal email should meet the set measures of the company.

On the other hand, contraction refers to a shortened form of a word that can act as a suffix when attached to another word. It also denotes the resulting word formed by combining these two words together (Truss, 2003). Hence, it is advisable to refrain from utilizing contractions in formal correspondences. Their use is deemed unsuitable in the context of formal legal writing. The fraudulent email from LandBank employed contractions, such as "don’t" and "it’s." In formal writing, these contractions should be spelled out by substituting them with their two-word equivalents.

1.7. Imperative Mood and Modality

An imperative mood serves to direct orders or instructions to individuals. Within the Imperative Sentence, there are two types: Commands, which involve instructions to carry out actions, and Prohibitions, which involve directives against specific actions or activities (Pauzan, 2021). Commands entail orders to perform an action, while prohibitions involve orders to refrain from performing certain actions (Hamzah, 2017). Scammers explicitly used imperative sentences, in LandBank email: ‘Please be advised that we will deactivate the access of your account's in LandBank Online Banking if we don't hear any actions from you,’ wherein the source text gives an order to the recipients of the message. Similarly, ‘You can verify your account at this link,’ and ‘please save this message for future reference’ in providing orders and instructions to the client. Azar & Hagen (2019) posit that modal verbs such as should, must, and can also be used in the imperative. In this case, the modal verb ‘can’ used by the scammer indicates the ability or possibility for the recipient to take action. It suggests that the recipient has the option or capability to verify their account at the provided link.

Moreover, the BDO scam email also contains imperative sentences: (a) ‘We are requiring you to please update and verify your personal information in our records’; the use of ‘requiring you’ indicates a mandatory action, while the inclusion of ‘please’ softens the request, making it more sound polite. (b) ‘Please verify your account from the link given below,’ this sentence is a direct request for the recipient to confirm or authenticate their account through a provided link, and it uses the word ‘please’ to make the request polite and respectful. Lastly, (c) ‘To complete, please fill out the verification form in our link,’ the same as with others; this is also a request instructing the recipient to fill out a verification form through the provided link. The word ‘please’ is used to request to sound courteous. Azar (2003) explains that imperatives are used for giving orders, instructions, suggestions, and invitations. It

is a grammatical mood used when the speaker has the authority to give orders or suggestions, and it can be used in different persons: second, first, or third person. Imperatives are also employed to persuade people to believe something that may not be true.

1.8. Flouting Grice's Maxims

Flouting a maxim occurs when a sender disregards the cooperative principle or its maxims but anticipates the receiver understands the implied meaning. This behavior involves acting against the cooperative principle, such as being dishonest or communicating in an unclear manner and can have negative consequences (Cutting, 2002). It results in individuals being unable to obtain the information they seek. For the LandBank email, the statement 'It's usually pretty easy to take care of things like this' may not directly contribute relevant information about the potential deactivation of the account access. This could be seen as a slight deviation from the maxim of relevance.

Moreover, the use of redundancy of the bank name (i.e., LandBank) and repetition of words and phrases (see Tautology) is deemed suspicious. This clearly violates Grice's Maxim, particularly the maxim of quantity. Similarly, in the BDO email, the message lacks specific details about the new anti-fraud system and the exact procedure for updating and verifying personal information. More specific information about the system and the verification process could enhance understanding. However, violating a maxim is prompted by certain causes and instances, as pointed out in the research carried out by Khosravizadeh & Sadehvandi (2011) State that violation of the maxim of quantity is mainly through redundancy, talkativeness, and circumlocution. Repetition of bank name clearly violates Grice's Maxim, particularly, the maxim of quantity that aims to persuade the client to believe that the source email is legit.

1.9. Suspicious Links

Fraudulent messages often mimic the appearance of renowned social media platforms, online auction sites, payment services, or IT administrators in order to trick unsuspecting individuals. Phishing emails often include links directing users to websites infected with malicious software (Bhavsar et al., 2018). Both emails display dubious links embedded with malware designed to redirect the email recipient to a counterfeit website resembling the official bank site. This tactic was expected to trick the recipient into authenticating themselves, a process known as phishing. The common form of phishing attack consists of an e-mail that is sent to numerous probable targets' mailboxes and that often contains a clickable link (Issac et al., 2014). The purpose is to fool the recipient of an email into thinking that the received email message is real and from the bank company. When the receiver clicks the hyperlink, the sender is linked or redirected to other fake websites and the attacker retrieves all the information that the receiver or user inputs into these websites (Wang et al., 2012).

Finally, this email appears to be more persuasive as it prompts the recipient to engage with them around the clock, as indicated in the fourth paragraph. A bank letter or an email can employ direct observing as well as indirect promoting skills (Insley, 2016). It should be used in neutral and positive correspondence as it is a direct approach to the subject. For negative communication, the use of indirect management is appropriate–potential non-transactions, cases of phishing, and similar situations should be dealt with in this manner. Similarly, towards the latter section of the email, the use of "important" appeared somewhat confusing. Employing "important" following a noun rather than a standalone word would be more explicit.

The change in the wording of all those email templates as a whole is significant but, in general, if the recipient of this email reacts 'positively', then it is okay. Otherwise, this can lead to the downloading of malicious software on the user's computer (Issac et al., 2014), in the end, getting the recipient's personal information leaving an open

window for more attacks. Understanding these details can serve as a precautionary measure and alert the recipients of scam emails in today's era of technological advancements. With online transactions becoming feasible, scammers are adapting to this trend by enticing users to open email attachments that mimic legitimate content. In other words, scam or fraudulent emails contain the following features: (1) Incorrect application of punctuation symbols, (2) Non-personalize salutations, (3) Redundant or repetitive use of words, (4) Improper application of apostrophes and contractions, (5) Uses imperative mood in persuading the recipient, and (6) Violates the Grice's Conversational Maxims.

2. Linguistic Features of Legitimate Emails

There is also a pattern of certain features of the scam emails that are easier to notice from the discourse structure (Onyebadi et al., 2012). However, one should understand the characteristics of the real email concerning the discourse and linguistics to differentiate it from a scam email so that the rate at which people fall anyhow to the fraudsters is minimized. Datar et al., (2014) mentioned that it is not always easy to identify scams and genuine emails as the latter are continually evolving.

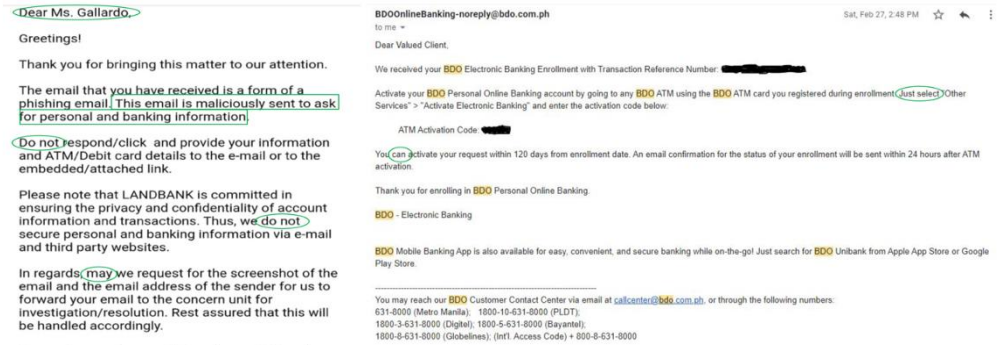
2.1. Correct Punctuation Markers: Comma

The email shown in Figure 2 is an authentic or legit communication from the LandBank of the Philippines. It serves as a bank case report, highlighting potential phishing or fraudulent activities from an unauthorized origin. Notably, the email displays adept formal writing and email skills. Unlike the email in Figure 1, this email correctly uses punctuation in the salutation by placing a comma after the recipient's name. According to Poudel (2010), punctuation plays a vital role in disambiguating the meaning of the sentence. This adheres to the customary conventions for composing a formal letter. The inclusion of a comma after the recipient's name in the "Dear <recipient name>" format was more formal and accurate in formal writing, as depicted in Figure 1 for comparison.

2.2. Non-repetitive Elements

The bank refrains from repeating or duplicating the company's name in the greetings, contrasting it with email 1 (refer to Fig. 1). Instead, in this instance, the bank's greeting was aimed at showing respect and deference to the email recipient. Despite the hidden email address, this email was considered legitimate to prevent participants from biasing their responses based on the email address (this concealment was for the email recipient's privacy). The presence of the company logo was sufficient evidence that validated the authenticity of this email (Chen & Guo, 2006), aside from relying solely on the bank's email address.

Figure 2 shows that the email address of the bank and the logo within the email were enough to ensure the receiver that the email originated from the bank. Contrary to Figure 1, in this instance, the scammer tries to persuade and reassure the client that the email originates from a trustworthy source. This attempt raised suspicion, signaling a potential scam. These two indicators served as initial signs that the email might be fraudulent.



Dear Ms. Gallardo,

Greetings!

Thank you for bringing this matter to our attention.

The email that you have received is a form of a phishing email. This email is maliciously sent to ask for personal and banking information.

Do not respond/click and provide your information and ATM/Debit card details to the e-mail or to the embedded/attached link.

Please note that LANDBANK is committed in ensuring the privacy and confidentiality of account information and transactions. Thus, we do not secure personal and banking information via e-mail and third party websites.

In regards, may we request for the screenshot of the email and the email address of the sender for us to forward your email to the concern unit for investigation/resolution. Rest assured that this will be handled accordingly.

BDOOnlineBanking-noreply@bdo.com.ph Sat, Feb 27, 2:48 PM

to me

Dear Valued Client,

We received your BDO Electronic Banking Enrollment with Transaction Reference Number: [redacted]

Activate your BDO Personal Online Banking account by going to any BDO ATM using the BDO ATM card you registered during enrollment. Just select "Other Services" > "Activate Electronic Banking" and enter the activation code below:

ATM Activation Code: [redacted]

You can activate your request within 120 days from enrollment date. An email confirmation for the status of your enrollment will be sent within 24 hours after ATM activation.

Thank you for enrolling in BDO Personal Online Banking.

BDO - Electronic Banking

BDO Mobile Banking App is also available for easy, convenient, and secure banking while on-the-go! Just search for BDO Unibank from Apple App Store or Google Play Store.

You may reach our BDO Customer Contact Center via email at callcenter@bdo.com.ph, or through the following numbers:
631-8000 (Metro Manila); 1800-10-631-8000 (PLDT);
1800-3-631-8000 (Digitel); 1800-5-631-8000 (Bayantel);
1800-8-631-8000 (Globelines); (Int'l. Access Code) + 800-8-631-8000

Figure 2. Legitimate Email

2.3. Avoidance of Contractions

Like in email 2, contractions are avoided in the communication called e-letter: for example, instead of writing "this email's" as in email 1 (see Fig. 1), the latter is written as "this email is" and "account's" was contracted. It is one of the common writing conventions that contractions are not used and these abbreviated words should be written out fully. In this e-mail, the writer avoids using 'do not,' though the writer from email 1 uses contractions like 'don't' and 'it's.' On the other hand, MLA allows the use of contractions in formal writing situations such as in publication and research. They established that the issue of when to apply the rule becomes easier once they have mastered the rule. Here are just a few: There are innumerable other situations where such close and formal style of writing where contractions are inappropriate; using contractions in such writing will sound impudent (Garner, 2009). Although the Modern Language Association (MLA) permits some flexibility with rules, in the context of the Philippines, it has been customary and traditional to avoid using contractions in formal letter writing. In this email, the writer adheres to the norms and complies with the regulations for composing a formal email.

2.4. Indicative & Imperative Mood and Modality

The indicative mood, known as the fact mood, is the most frequently used among the three moods. It is utilized to state facts, describe actual events, or convey actions. This mood finds application in making statements, asking questions based on facts, or expressing exclamations related to factual information (Gu, 2022). In this case, the legit emails used indicative declarative mood, particularly the statement of facts. For example, 'The email that you have received is a form of a phishing email.' This sentence provides information about the nature of the email received from the scammer. Similarly, the statement 'please note that LANDBANK is committed in ensuring the privacy and confidentiality of account information and transactions' this sentence informs the reader about LANDBANK's commitment to data security. In other words, these sentences state facts, describe situations, or present information without giving commands or making requests, unlike scam emails. The content is straightforward statements aiming to inform or describe rather than direct action.

The imperative mood, known as the will mood, pertains exclusively to future actions and serves to issue commands, offer advice, make requests, and express one's will, among other directives. It exists solely in a simple form, employing the plain root form of the verb without any inflection, applicable to the second person singular or plural (Gu, 2022). In this case, legitimate emails, compared with scam emails, use advice and commands in navigating and activating bank accounts, while scam emails use imperative mood only. For instance, 'Activate your BDO Personal Online Banking account by going to any BDO ATM using the BDO ATM card you registered during enrollment.' this sentence is a directive instructing the recipient to take action: activating their BDO Personal Online Banking account by visiting any BDO ATM and using the BDO ATM card previously registered during the enrollment process. Moreover, the sentence 'Just select 'Other Services' > 'Activate Electronic Banking' and enter the activation code below' this sentence is another set of instructions guiding the recipient on specific steps to follow: selecting certain options to activate the electronic banking service.

The use of modal auxiliary verbs as manipulative and deceptive strategies in scam emails (Chiluwa & Anurudu, 2020). In this study, the legit email used the English modal auxiliary verb 'can' in the sentence 'You can activate your request within 120 days from enrollment date,' this modal verb expresses the ability or possibility for the recipient to perform the action of activating their request within a specific timeframe than the scam email that specified 24/7. In addition, Chiluwa & Anurudu (2020) posit that the most frequent modal verb 'may'

from legit emails, signal politeness and scam emails used the verb 'can' as their hedging strategies to obligate the recipient to perform such actions.

Finally, in the second email, a deliberate use of indirect and persuasive strategies was observed. This approach may seem contradictory compared to the first email, but the circumstances differed in this case. It was a phishing report from the receiver informing the authenticity of the funds received indirectly to the bank company (Furnell, 2007). It includes adverse details about the deceitful email aimed at phishing personal and banking data. Simultaneously, the writer employed a persuasive approach, attempting to influence the email recipient. This persuasive tone was evident in the negative phrasing advising "do not respond/click," which aimed to sway the recipient. Similarly, the usage of "may" was employed as a request or to indicate possibilities regarding the screenshot for obtaining evidence from the scam email.

2.5. No Third Party Website

Amid the prevalence of phishing and online fraud, legitimate emails clearly notify the message recipient that the bank will not send any links directing them to counterfeit websites. These emails also explicitly advise against clicking on any suspicious links or providing bank-related information like ATM/Debit card details in response to such emails. Instead, the bank explicitly labels this as a malicious threat, as depicted in Figure 1. Moreover, the case in email 1 can be categorized as phishing by fraud based on the criteria set by Issac et al. (2014). It compromised its users through emails because most of the emails sent to the users were fake and thus they were forced to reveal their passwords, bank account numbers, contact details, PINS, and many others.

In general, deceptive and fraudulent emails have the potential to pilfer secretive information from users, leading to financial losses and compromising financial data. Discerning the disparities between a scam and a genuine email is crucial, even when subtle indicators are present. Overlooking these factors may seriously affect the advancement of electronic commerce in the cyber world which can lead to the erosion of confidence and trust in using the internet (Drake et al., 2004). Analyzing particular aspects may help the users avoid fraudsters and scammers and, therefore, protect themselves. These features might encompass deceptive sender addresses, logos (such as color, shapes, fonts, and style), as well as fake web links found in emails. The escalation of awareness among users is essential to counter the very complex and well-organized fraudulent activities that exist freely in the context of cyberspace.

Table 1. Summary of the Language of Emails

Scam Emails	Legitimate Emails
• Faulty Punctuation Markers • Non-personalize Salutations • Repetition and Redundancy • Orthographic and Indentation Errors • Apostrophes and Contractions • Imperative Mood and Modality • Flouting Grice's Maxims • Suspicious Links (Third-Party Website)	• Correct use of Punctuation Markers • Non-repetitive Elements • Avoidance of Contractions • Indicative and Imperative Modality • No Third-Party Website

CONCLUSION

This research quite comprehensively explores the semantics required for filtering out the emulators and the arrival of real/original or genuine emails. With the precedence of new technology's relation between the individual and the bank especially via the Internet, Email has become one of the most important mediating tools. However, technological growth has also brought about negative aspects in that various criminals have in their vice used

emails for con activities. It is always a challenge to be able to distinguish between the real and the fake, especially in emails. The objective of this particular research is to define potential discrepancies most often overlooked and features making the e-mail a phishing one. With these indicators, it is assumed that regarding the number of reported cases the amount of actual phishing attacks could go down, which aids people in differentiating scams from actual emails in the inbox or spam folder. The body of literature reveals that there are strategies to build models that categorize scam emails by content and characteristics. This is a criterion where a significant difference between the fake sender and a real representative is made through the use of the email domain. Typically, one would expect to find spelling mistakes, typographical errors, contractions, and unnecessary repetitions in scam emails, indents and structures in the emails are distorted. Normal links most of the time direct the user to look-alike websites, where personal details will be obtained. Forces are aggressively used to make users click on certain links that are misleading in nature by the scammers. It is to prevent this that user education is important. The client who does not have awareness or knowledge has issues that include the following even though the organization's defense mechanisms may be considered advanced.

On the other hand, actual emails are punctually correct, no contraction is used, and repetition is avoided. Bank emails are contractual and official thus, they do not contain any links that are considered to be damaging. They employ authentic senders' email domains linked with genuine banks and do not have any spelling mistakes; in addition, they have appropriate indents. Real-life emails set an indicative tone and directly state something or use other direct ways of conveying information. To prevent the occurrence of such scams in the first place, therefore, the language used in these scams as well as those used in legitimate emails should be well understood. Noting these slight signs can prevent instances of phishing, although just educating the users is insufficient. Over time, evolution in technology leads to better work done by the con artists and better and more imitating emails sent out. User education and following the indicators act as antecedents and can be considered preventive measures for any client to be on the lookout for any email scams and financial losses. The criminals never stop in emulating the look and feel of the bank emails. Therefore, banks and other acting businesses should follow the best practices for emails to be able to notice and report scams received in their mail.

Declaration by Authors

Acknowledgement: None
Source of Funding: None
Conflict of Interest: The authors declare no conflict of interest.

REFERENCES

1. Ali Taha V., Pencarelli T., Škerháková V., Fedorko R., Košíková M. (2021). The use of social media and its impact on shopping behavior of Slovak and Italian consumers during COVID-19 pandemic. Sustainability, 13, 1710. https://doi.org/10.3390/su13041710
2. Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science, 3, 1-23. https://doi.org/10.3389/fcomp.2021.563060
3. Al-Marsumi, N. H. R. (2017). The use of tautology in "The Thorn" by William Wordsworth: A stylistic study. AWEJ for Translation and Literarcy Studies, 1(3), 139-161. DOI: http://dx.doi.org/10.24093/awejtls/vol1no3.10
4. Almomani, A., Gupta, B., Atawneh, S., Meulenberg, A., & Almomani, E. (2013). A survey of phishing email filtering techniques. IEEE Communications Surveys and Tutorials, vol. 15, no. 4, pp. 2070-2090, doi: 10.1109/SURV.2013.030713.00020.
5. Altalhab, S. (2018). Short- and Long-term effects of repetition strategies on vocabulary retention. Advances in Language and Literary Studies. Vol. 9, 2, pp. 146-149. ISSN: 2203-4714

6. Azar, B. S. (2003). Fundamentals of English Grammar. Longman.
7. Azar, B. S., & Hagen, S. A. (2019). Fundamentals of English Grammar: Pearson Practice English App. Pearson Education.
8. Bhavsar, V., Kadlak, A., & Sharma, S. (2018). Study on phishing attacks. International Journal of Computer Applications, 182(33), 27-29. DOI: 10.5120/ijca2018918286
9. Blommaert, J., & Omoniyi, T. (20016). Email fraud: Language, technology, and the indexicals of globalization. Social Semiotics, 16(4), 573-605. DOI: 10.1080/10350330601019942
10. Brennan, M. (1992). Techniques for improving mail survey response rates. Marketing Bulletin, 3, 24–37.
11. Chen, J., & Guo, C. (2006). "Online detection and prevention of phishing attacks," in in Proc. Fifth Mexican International Conference in Computer Science, IEEE Conference, pp. 1-7.
12. Chiluwa, I. M., & Anurudu, S. (2020). Expressing (un)certainty through modal verbs in advance fee fraud emails. Covenant Journal of Language Studies, 8(1), 17-34.
13. Collins, J., Hammond, M., & Wellington, J. (eds) (1997). Teaching and Learning with Multimedia. London: Routledge.
14. Crismundo, K. (2021). Digital fraud attempts in PH rise amid pandemic. Philippines News Agency. https://www.pna.gov.ph/articles/1134735
15. Cutting, J. (2002). Pragmatics and Discourse: A Resource Book for Students. New York: Routledge.
16. Datar, T., Cole, K., & Rogers, M. (2014). Awareness of Scam E-mails: An Exploratory Research Study. Annual ADFSL Conference on Digital Forensics, Security and Law. 12. https://commons.erau.edu/adfsl/2014/wednesday/12
17. Diaz, A., Sherman, A. T., & Joshi, A. (2020). Phishing in an academic community: A study of user susceptibility and behavior. Cryptologia, 44(1), 53–67.
18. Dillman, D. A. (2000). Mail and Internet surveys: The tailored design method (2nd ed.). New York, NY: John Wiley & Sons.
19. Drake, C., Eugene, J., & Koontz, A. (2004). "Anatomy of a Phishing Email," in First Conference on Email and Anti-Spam (CEAS), Mountain View, CA, USA.
20. Freiermuth, M. (2011). Text, lies and electronic bait: An analysis of email fraud and the decisions of the unsuspecting. Discourse and Communication, 5, 123-125. Doi: 10.1177/1750481310395448
21. Furnell, S. (2007). An assessment of website password practices. Computer Security. 26, 445–451. doi: 10.1016/j.cose.2007.09.001
22. Garner, B. (2009). Garner's Modern American Usage. Oxford UP.
23. Gu, W. (2022). Mood expression for ESL students. West Career & Technical Academy. Retrieved from https://files.eric.ed.gov/fulltext/ED619632.pdf
24. Hassan, A., & Barber, S.J. The effects of repetition frequency on the illusory truth effect. Cognitive Research 6, 38 (2021). https://doi.org/10.1186/s41235-021-00301-5
25. Insley, R. (2016). Business Letters & Memos from Communication in Business (2nd ed.). Kendal Hunt Publishing. Pp. 291-333.
26. Issac, B., Chiong, R., & Jacob, S.M. (2014). Analysis of Phishing Attacks and Countermeasures. ArXiv, abs/1410.4672.
27. Kavrestad, J., Hagberg, A., Nohlberg, M., Rambusch, J., Roos, R., & Furnell, S. (2022). Evaluation of contextual and game-based training for phishing detection. Future Internet 2022, 14(4), 104; https://doi.org/10.3390/fi14040104
28. Khosravizadeh P., & Sadehvandi, N. (2011). Some instances of violation and flouting of the maxim of quantity by the main characters in Dinner for Schmucks. International Conference on Languages, Literature and Linguistics. Singapore: IACSIT Press.
29. Kim, D., Yoon, H. B., Yoo, D., Lee, S., Jung, H., Kim, S. J., Shin, J., Lee, S., & Yim, J. (2016). Etiquette for Medical Students' Email Communication with Faculty Members: A Single-Institution Study. BMC Medical Education, 16, 129. https://doi.org/10.1186/s12909-016-0628-y
30. Lugtu, R. (2021). Shifts in digital marketing. The Manila Times. https://digitaledition.manilatimes.net/manila-times
31. Onyebadi, U., & Park, J. (2012). 'I'm Sister Maria. Please help me': A lexical study of 4-1-9 international advance fee fraud email communications. International Communication Gazette, 74(2), 181–199.
32. Lasota, J. (2008). The apostrophe revisited: Attitudes, errors and implications for

teaching in an upper secondary school (Published Thesis). Institutionen for humaniora och samhallskunskap. Retrieved from https://www.diva-portal.org/smash/get/diva2:221793/FULLTEXT01.pdf
33. Pomorska, K. (1987). Language, Poetry and Poetics. Amsterdam: Mouton.
34. Poudel, S. S. (2010). A study on the use of punctuation in guided and essay writing (published thesis). Prithivi Narayan Campus, Pokhara. Retrieved from https://elibrary.tucl.edu.np/bitstream/123456789/4941/1/THESIS.pdf
35. Ragucci, J., & Robila, S. (2006). Societal Aspects of Phishing. IEEE, 1-5. Doi: 10.1109/ISTAS.2006.4375893
36. Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. Future Internet, 11, 89.
37. Schaffer, D. (2012). The language of scam spams: Linguistic features of 'Nigerian Fraud' e-mails. A Review of General Semantics, 69(2), 157-179.
38. Shannon, L., & Bennett, J. (2011). A case study: Applying critical thinking skills to computer science and technology. Information Systems Educators Conference, 28.
39. Truss, L. (2003). Eats, shoots & leaves: The zero tolerance approach to punctuation. Suffolk, NY: Gotham Books. Retrieved from https://www.weizmann.ac.il/oc/martin/esl.pdf
40. Unkelbach, C. (2007). Reversing the truth effect: Learning the interpretation of processing fluency in judgments of truth. Journal of Experimental Psychology: Learning, Memory, and Cognition, 33, 219–230. https://doi.org/10.1037/0278-7393.33.1.219
41. Unkelbach, C., & Greifeneder, R. (2013). A general model of fluency effects in judgment and decision making. In C. Unkelbach & R. Greifender (Eds.) The experience of thinking: How the fluency of mental processes influences cognition and behavior (pp. 11–32). New York, NY: Psychology Press. https://doi.org/https://doi.org/10.4324/9780203078938
42. Unkelbach, C., & Stahl, C. (2009). A multinomial modeling approach to dissociate different components of the truth effect. Consciousness and Cognition, 18, 22–38. https://doi.org/10.1016/j.concog.2008.09.006
43. Wang, J., Herath, T., Chen, R., Vishwanath, A., & Rao, H. R. (2012). Phishing susceptibility: An investigation into the processing of a targeted spear-phishing email. IEEE Transactions on Professional Communication, 55(4), 345–362.

How to cite this article: Sophomore T. Vacalares, Brian Paul E. Sta. Ana, Daryl Q. Dranto, Jinky S. Gallano. Bank emails: the language of legit and scam. *International Journal of Research and Review*. 2024; 11(7):192-203. DOI: *https://doi.org/10.52403/ijrr.20240721*

******