“Your account has been compromised” Exploring emotional triggers in scam emails

"Your account has been compromised"

Exploring emotional triggers in scam emails

Mostafa Morady Moghaddam and Erhan Aslan
Shahrood University of Technology | University of Reading

Scam emails pose a significant threat to online security, exploiting individuals' vulnerabilities through emotional manipulation. This study explores emotional triggers in a corpus of scam emails ($n = 371$) compiled from ten genuine email accounts over a period of five years (2018–2023). Using Robinson's (2008) taxonomy of *basic emotions*, the positive and negative emotional content and triggers were identified and analyzed. The findings reveal that an overwhelming majority of the emails allude to negative emotions ($n = 252$), suggesting a clear scammer strategy in stimulating negativity to achieve fraudulent objectives. Conversely, the emails that evoke positive emotions ($n = 119$) seem to create a false sense of trust, sociability and gratitude. In addition, many scam emails employ various combinations of emotional triggers to manipulate recipients. This study sheds light on the intersection between emotions and discourse pragmatics and highlights the affective dimensions of discourse in email communication.

Keywords: discourse pragmatics, emotional triggers, scam emails, social psychology, cybersecurity

1. Introduction

Since the dawn of email communication, spam has compromised the privacy of users by exploiting their personal information. In 2018 alone, at least 14.5 billion spam emails were recorded (Karim et al., 2019). According to the FBI, spam-related attacks caused financial losses to businesses amounting to approximately $ 257 billion between 2012 and mid-2020 (Karim et al., 2019). Chiluwa (2019) reported that the losses arising from scam emails totaled $ 12.7 billion in 2013, and individuals from the US, UK, and India were the primary victims. In 2023 alone, 145.5 million American consumers were reported to have been affected by spam

https://doi.org/10.1075/ip.00135.mog | Published online: 4 March 2026
Internet Pragmatics ISSN 2542-3851 | E-ISSN 2542-386X

attacks that involved stolen personal information such as birthdates, credit card details, social security numbers (Febriyani et al. 2023).

Scam emails are a form of phishing, a fraudulent practice that often uses forged emails or websites to deceive users into disclosing personal information (Daintith and Wright 2008). The goal of scam emails is to style messages in such a way as if they have been sent genuinely (Blommaert and Omoniyi 2006; Blanzieri and Bryl 2008; Kwak et al. 2020) under the guise of attempting the recipient of the email to perform an action for an ingenuine reason (Wash 2020). Some of these actions involve the recipient to click a link or open a file that would lead to the downloading of malicious software to collect sensitive personal information from the victim's computer (Norris and Brookes 2021). Scam emails exhibit three main features: a) they are unsolicited; b) they are received from unknown senders; and c) they ask for personal information or require the addressee to reveal their personal identity or take some action.

Scam emails are on the rise globally, facilitated by technology that enables fraudsters to impersonate legitimate communications (Tambe Ebot et al. 2024). In this regard, Norris and Brookes (2021: 1) argue that "the growth in social communication facilitated by technology mean that online scams represent a growing societal issue, with perpetrators successfully persuading people to make fraudulent payments or download malicious attachments." As the number of registered internet companies continues to grow, the complexity of fraud has also increased. This complexity is particularly evident in the content of scam emails (Safaei Pour et al. 2023). Email is considered a less-rich medium, making it less effective at conveying feedback, nonverbal cues, voice, and emotions (Keil and Johnson 2002). Therefore, detecting deception in emails is often more challenging than in messages communicated through richer media channels, such as face-to-face interactions or phone calls. Consequently, emails have become a primary medium for scam attacks, involving the illicit harvesting of addresses to promote fraudulent or worthless products (Khan et al. 2015).

Scam emails serve two primary purposes, as noted by Shaw (2008: 270): overtly, they offer a profitable but questionable deal from which both parties may benefit; covertly, they aim to trick the recipient, providing no benefit at all. Scam emails include various types of deception, such as advance-fee scams that promise a large sum of money in exchange for a smaller upfront payment (Chawki 2009), lottery scams which inform recipients that they have won a lottery or prize and must pay a fee to claim it (Bourne et al. 2013), investment scams which offer too-good-to-be-true investment opportunities (Naylor 2007), romance scams which seek online relationships to solicit money (Sorell and Whitty 2019), charity scams that solicit donations for fake charities, particularly after disasters (Fredericks and

Rowe 2016), and impersonation scams, where the sender pretends to be someone else, such as a relative in need or a government official (Vilardo 2004).

The emergence of diverse web-based communication applications has led to the creation of numerous forms of digital expressions of emotions in instant messaging or chat, such as emoticons, emojis, and stickers to aid emotional expression and understanding (Alkhalil et al. 2021). Spending considerable time on digital media, we are also exposed to expressions of emotions by other people leading to *emotional contagion*, a term originally defined by Hatfield, Cacioppo and Rapson (1993: 96) as "the tendency to automatically mimic and synchronize expressions, vocalizations, postures, and movements with those of another person's and, consequently, to converge emotionally." Other scholars like Goldenberg and Gross (2020) describe the kind of emotional contagion observed on digital platforms as *digital emotional contagion*, which is more frequent and intense than emotional contagion observed in non-digital contexts.

Much of what we consume on digital platforms is negative with unfavorable effects on our lives, directly or indirectly (Pellegrino, Abe and Shannon 2022). Negative content may have harmful effects on privacy, well-being and functioning, equality, social relations and social cohesion, making individuals more vulnerable to scam attacks (Shadel and Pak 2007). Although technological solutions and user awareness campaigns have been instrumental in mitigating scam attacks, they often overlook the emotional aspects of such scams. By incorporating insights from the fields of emotions and discourse pragmatics, this study attempts to bridge the gap between traditional cybersecurity approaches and the nuanced understanding of emotional manipulation techniques employed by attackers.

Scam emails maintain their effectiveness as the strategies in their construction are frequently updated (Genc et al. 2021). Attackers strategically exploit recipients' emotional vulnerabilities to manipulate their actions and increase the likelihood that recipients will fall victim to scams (Vishwanath et al. 2011). Emotions have long been recognized as powerful motivators of human behavior, influencing decision-making processes and shaping interpersonal interactions (Morris and Keltner 2000). Understanding the emotional triggers employed by attackers is crucial for developing effective interventions and countermeasures (Silic and Back 2016). As Korpela (2015) emphasizes, it is crucial to identify mechanisms for protection against email scams, and it is a good practice to provide education and knowledge to identify such fraud. The success or failure of a scam email is determined by the reaction of the recipients, and the recipients' decisions to click on a link or open an attachment can be affected by how effective a phisher may trigger different emotions from the victims (Alkhalil et al. 2021). Emotions play a significant role in recipients' responses to emails often clouding judgment about the legitimacy of the intended message (Jayatilaka, Arachchilage and Abar 2021).

Therefore, to gain a deeper understanding of how scam attacks operate on digital platforms, it is essential to consider the significant role that emotions play in contemporary digital discourse and communication practices (Karamagi 2022; Dutt 2023).

The theoretical underpinnings of the present study lie in the integration of emotions, discourse pragmatics, and cybersecurity. By examining the interplay between these fields, this study aims to contribute to a comprehensive understanding of scam attacks and provide valuable insights to enhance individuals' online security in an increasingly interconnected world. Against this background, this study addresses the following questions:

1. What are the positive and negative emotions observed in scam emails?
2. What are the possible combinations of different emotional triggers in scam emails?

To situate the present study in view of the extant research on scam emails, we provide an overview of the linguistic and discourse features of scam emails as they pertain to persuasion. Later, we discuss the emotional triggers associated with scam emails, the focus of the present study, followed by the methodology and findings.

2. Literature review

2.1 Linguistic and discourse features of scam emails

Research on scam emails is diverse and multifaceted. Some studies have focused on the syntactic characteristics of scam emails. For instance, by exploring the cues that deceptive senders use, Zhou et al. (2003) identified the dominant use of ellipsis, wordy sentences, and passive voice construction in scam emails. Other scholars have found inconsistent punctuation and use of informal style (Blommaert and Omoniyi 2006) and inappropriate capitalization and spelling/grammar errors in scam emails (Holt and Graves 2007), which suggest that the literacy skills of the writers are very poor. Investigating the pragmatic act of phishing in a corpus of 100 scam messages, Tseng (2010) found both direct and indirect uses of directives. Bernal and Belli (2013) identified gendered language in fraudulent emails. In their study, scam email writers who presented themselves as female produced more emotional and affectionate words than their male counterparts, and male-sender scam emails were mostly concerned with business or financial transactions. Analyzing 40 scam emails, Anafo and Ngula (2020) found that scam emails tended to be interpersonally rich in the use of personal pronouns to index and

position scammers relative to their target email recipients in manipulative ways. That being the case, the crafting of scam emails is associated with social variables, such as gender, power, and register, which likely contribute to the susceptibility of recipients to deception.

Research has also shown that individuals tend to focus on the most noticeable elements of scam emails by evaluating the text (Stojnic, Vatsalan and Arachchilage 2021). These elements refer to the key features that stand out, such as the overall layout, wording, and any highlighted information. Additionally, biases and heuristics in terms of the reliability of a message source, whether the material violates expectations, also affect recipients' judgments (Metzger, Flanagin and Medders 2010). However, by increasing the sophistication of scam emails in their structure and the inclusion of implicit meaning, scam emails can have a better chance of reaching their intended purpose (Nadeem et al. 2023).

Other studies have focused on the discourse features of scam emails including persuasive and manipulative strategies (Ajayi 2022) and opening and closing moves (Freiermuth 2011). Analyzing the discursive-pragmatic contents and structures of scam emails, Chiluwa (2009) found that writers applied sociocultural greeting formulas, reassurance, and confidence building as well as action-prompting strategies to sustain receivers' interest. Vishwanath, Harrison and Ng (2018) investigated the effect of persuasive techniques on scam susceptibility using a unified information processing model. Persuasive techniques are included in the content of emails to encourage users to react accordingly. The scam emails conveyed a sense of urgency by drawing on time-limited offers or deadlines, offering prizes, or signifying that failure to respond would probably cause a loss (Sillence et al. 2006). Although Vishwanath, Harrison and Ng (2018) did not identify any differences in susceptibility to emails containing reward-based versus threat cues, the psychological concept of loss aversion suggests that people are more sensitive to possible losses than gains. As a result, scam emails that refer to potential losses could be much more tempting than those describing potential rewards (Parsons et al. 2019). To determine the trustworthiness of emails, people typically use external cues, considering the 'feel and look' of the information (Sillence et al. 2006). In another study, Chiluwa (2019) highlights the emotional appeals to the receiver in the conclusion of scam emails in which religious tones or sentiments are evoked and a story of sudden death is sometimes shared.

The existing research has also revealed that the common characteristics of scam emails include structural properties such as misleading hyperlinks and header information (Naqvi et al. 2023; Safi and Singh 2023). To make a scam email effective, its content requires the intended victim to act urgently; for example, an email that informs the recipient of account termination if the recipient does not respond or perform an action within a limited time. To obtain compliance from

the recipient of a scam email, persuasive strategies and emotional triggers are used to elicit a positive response from the intended victim (Workman 2008).

2.2 Emotional triggers in scam emails

As discussed earlier, emotions play a significant role in today's digital communication shaping and affecting digital discourse and communication practices. The importance of emotion perception in emails has increased in recent years (Blunden and Brodsky 2021). Scammers often manipulate emotional triggers to fulfill their fraudulent intentions (Jayatilaka, Arachchilage and Abar 2021). Emotional triggers are often specific events or stimuli that elicit immediate reactions. These reactions can be classified as basic emotions, transient experiences resulting from interactions with the environment or memories of past events (Kensinger and Ford 2020). For example, if a person has previously experienced joy from a particular activity, the emotional trigger associated with that activity may lead them to engage in the activity again. Robinson (2008: 115) argues that positive and negative emotions can "refer to mental experiences with strongly motivating subjective qualities akin to the basic sensations of either pleasure or pain." For example, positive emotions like 'attraction' or 'desire' can lead to behaviors aimed at seeking contact or engaging with beneficial environments, while negative emotions such as *alarm* and *fear* can result in avoidance or defensive behaviors (Shadel and Pak 2007).

There is a scarcity of research exploring emotional triggers in scam emails (Jonas, Graupmann and Frey 2006; Cukier, Nesselroth and Cody 2007). Consequently, not many people are aware of the existence of emotional triggers in emails they receive (Blunden and Brodsky 2021). Emotional triggers can be effectively exploited in scam emails to manipulate recipients into taking actions that benefit the scammer. Current scam email countermeasures largely rely on technical aspects (Almomani et al. 2013) which include technological measures and tools used to detect and prevent scam emails (Aleroud and Zhou 2017), such as spam filters, antivirus software, and algorithms that analyze email metadata and patterns. These measures primarily focus on identifying suspicious characteristics based on coding, formatting, and known scam patterns, without considering emotional triggers that scammers exploit to manipulate recipients.

Despite the existing literature on the linguistic features and technical countermeasures against scam emails, our understanding of how psychological aspects, particularly emotional triggers such as fear and greed, are embedded within these scams is limited (Cukier, Nesselroth and Cody 2007). Freiermuth (2011: 127) highlights the importance of this perspective, arguing that "it is imperative to establish a framework that considers what elements cause people to change their minds." A

possible answer to this concern can be found in the realm of emotional triggers. Research findings indicate that individuals who have been scammed often experience a range of negative emotions, including shame, anger, regret, betrayal, helplessness, embarrassment, sadness, and depression (Shichor et al. 1996; Fischer et al. 2005; Jonas et al. 2006). In this regard, Norris and Brookes (2021: 1) mention that "there is limited examination of the context or state induced factors, such as emotional state of the individual, and, importantly, how that may impact upon their decision making process." This limits the development of comprehensive strategies that enhance user awareness and resilience against such deceptive practices. Therefore, further research is required to integrate insights from psychology and cybersecurity measures to address this critical gap.

In the realm of psychology and behavioral science, understanding the intricate interplay between emotions, triggers, and human behavior is paramount (Dirwan and Latief 2023). Emotions serve as powerful motivators that significantly influence decision-making processes and actions (Lerner et al. 2015). The purpose of the present study is to explore the mechanisms through which emotional triggers may affect behavior, particularly in contexts where individuals may be vulnerable to manipulation, such as scam emails. By examining the underlying emotional dynamics and their implications in scam emails, we can gain valuable insights into how emotions shape our responses to various stimuli and the potential consequences of these responses.

3. Methodology

3.1 Data

The data collection in this study involved a systematic approach to gathering scam emails. The emails were compiled from 10 different accounts created specifically for research over a period of 5 years, from 2018 to 2023. These accounts were not associated with real participants; instead, they were established solely to collect data on email communications, with scam emails sent directly to these accounts. We had full access to these accounts during the data collection period. In academic research, it is common practice to use anonymized data or research-specific accounts to ensure privacy and uphold ethical standards (Wiles et al. 2008). This method allows a diverse and representative sample of scam emails to be analyzed, providing valuable insights without compromising individual privacy. The types of scam emails received during the data collection period included a variety of common scams, such as phishing emails, investment fraud, lottery scams, and Nigerian Prince scams.

The scam emails were primarily in English. However, a few emails received were written in languages other than English, reflecting the global nature of scam operations. These non-English emails were excluded from the analysis. To ensure dataset integrity, duplicates sent to different accounts were discarded. This was crucial to avoid skewing the results with repetitive data that could misrepresent the prevalence of specific emotional triggers. Additionally, other filtering criteria were applied, such as excluding emails that were clearly not scams (e.g., legitimate marketing emails) and those that lacked substantial emotional content. Emails that were too vague or generic and lacking identifiable emotional triggers were also excluded from the final analysis.

3.2 Framework and data analysis

The analysis of the data was based on Robinson's taxonomy of basic emotions (see Table 1) which facilitated a comprehensive and systematic categorization of emotions, distinguishing between positive and negative emotional experiences. This dual categorization is particularly relevant in the context of scam emails, where understanding the specific emotional appeals used by scammers can illuminate their manipulative strategies. By using this taxonomy, we could effectively identify and analyze the emotional content of scam communications, leading to more nuanced insights into how these emotions influence decision-making processes. In addition, Robinson's taxonomy is grounded in psychological research, which lends credibility to its application in understanding emotional triggers.

The thematic analysis conducted in this study involved several key procedures to ensure a comprehensive understanding of the emotional triggers in scam emails. The first step was to classify the emotional triggers in scam emails as either positive or negative and assigning them to the emotion category proposed by Robinson (2008). We immersed ourselves in the data by reading and rereading the scam emails to gain a deep understanding of the content. The next step was to identify and group the codes representing significant features of the data related to positive and negative emotional triggers. To name these codes, eleven pairs of positive and negative emotions proposed by Robinson (2008: 155) were used (Table 1). The identified themes were reviewed and refined to ensure they accurately represented the data and were distinct from one another. The themes identified in this study are shown in Figures 1 and 2.

To ensure that each emotion was coded and identified appropriately, we followed the definitions of emotions in Robinson's (2008: 157–159) framework. For example, Robinson (2008: 159) defines 'alarm' as "unlearned signals of immediate and extreme danger, such as very intense stimulation." In addition, Robinson (2008: 159) defines 'gratitude' as "acts of kindness, mercy, assistance and co-

Table 1. Robinson's (2008: 155) taxonomy of eleven pairs of positive and negative emotions

Type of emotion	Positive emotions	Negative emotions
Emotions related to object properties	Interest, curiosity	Alarm, panic
	Attraction, desire, admiration	Aversion, disgust, revulsion
	Surprise, amusement	Indifference, familiarity, habituation.
Future-appraisal emotions	Hope	Fear
Event-related emotions	Gratitude, thankfulness.	Anger, rage
	Joy, elation, triumph, jubilation	Sorrow, grief
	Relief	Frustration, disappointment
Self-appraisal emotions	Pride in achievement, self-confidence, sociability	Embarrassment, shame guilt, remorse
Social emotions	Generosity	Avarice, greed, miserliness, envy, jealousy
	Sympathy	Cruelty
Cathected emotions	Love	Hate

operation done by another." The data were coded by a trained research assistant to ensure the reliability of the coding procedure. We used intercoder reliability to measure the amount of agreement among the independent coders. Cohen's Kappa of 0.87 showed a high level of agreement. Table 2 presents some coding examples.

Table 2. Examples of the coding procedure

Email ID	Trigger phrase	Emotion category	Specific emotion
001	"Your account will be suspended unless you act now."	Negative	Fear
002	"Congratulations! You've won a prize!"	Positive	Joy
003	"My late parents died during the political war."	Negative	Sorrow

In the analysis, raw frequencies and percentages were computed to provide a quantitative overview of the emotional triggers identified in the dataset. Raw frequencies were calculated by counting the total number of instances of each emotional trigger across the sample of scam emails. Subsequently, percentages were derived by dividing the raw frequency of each emotional trigger by the total number of analyzed emails, allowing for a clearer understanding of the prevalence of

each trigger relative to the entire dataset. Regarding the handling of combinations of emotional triggers, each email was analyzed for the presence of emotional triggers, and instances of combinations were counted separately as distinct groups. This means that if an email contained multiple emotional triggers, it was counted once in the overall total for each individual trigger category (e.g., alarm, fear, greed) and counted once as a combination. For example, if an email exhibited both 'alarm' and 'fear', it would contribute to the raw frequency counts for both 'alarm' and 'fear' as individual triggers, as well as being counted as an instance of a combination of emotional triggers. This dual counting approach allows for a more nuanced understanding of how often specific combinations are used in scam emails while maintaining the integrity of individual trigger counts.

4. Findings

4.1 Quantitative analysis of data: Negative and positive emotional triggers

Table 3 highlights the emotional triggers identified in scam emails, focusing on both negative and positive emotions. The table illustrates that negative emotions are prevalent in scam emails, with 'alarm' being a particularly dominant trigger. This suggests that scammers often employ tactics that evoke a sense of urgency or fear to convince recipients to act quickly without critical evaluation. Although positive emotions are present, they are less frequently observed than negative emotions. This highlights the strategic focus of scammers on inducing fear and urgency rather than fostering positive feelings.

Table 3. The main emotional triggers found in scam emails

Emotional triggers	Sample message content	Frequency	Percentage
Negative emotions			
Alarm	I would like you to contact me via email for further details as this is a very sensitive issue that requires urgent attention from you.	93	25%
Fear	The Banking law and guidelines here stipulate that if such money remained unclaimed after nine years, the money will be transferred into the Bank treasury as unclaimed fund.	53	14%
Sorrow	My late parents died during the political war in my country in 2011.	42	11%

Table 3. *(continued)*

Emotional triggers	Sample message content	Frequency	Percentage
Greed	Note that you will have 45% of the above sum if you agree to handle this business with me, while 50% will be for me and after this transaction, 5% will remove any expenses that may arise during the process.	33	9%
Guilt	I grew up as an orphan, and I don't have anybody as my family member. So, I am expecting your response.	31	8%
Subtotal		252	67%
Positive emotions			
Sociability	I am looking for a long term relationship and investment assistance.	28	8%
Surprise	I know that this letter will come to you as a surprise as we have never met before.	24	7%
Trust	I will send to you a copy of my international passport which you will show to the bank to make the bank know that I instructed you to contact them for the transfer of my fund.	19	5%
Gratitude	I appreciated your efforts at that time very much.	18	5%
Generosity	I want to donate my inherited ($ 10.7 Million dollars) to you so that you can use the money for humanitarian aid and charitable works.	15	4%
Relief	May Allah give you peace of mind.	9	2%
Self-confidence	Our company has offices in major ports in China and always provides the best service for import and export by sea and air.	6	2%
Subtotal		119	33%
Total		**371**	**100%**

The prevalence of negative emotions in scam emails is striking, with 252 instances observed in the sample (considering the sum of the first five emotions in Table 3, which are negative emotions). On the other hand, the occurrence of positive emotions in scam emails, though less frequent with 119 instances, demonstrates scammers' attempt to establish trust, build personal connections, and trigger recipients' altruistic responses. Figures 1 and 2 illustrate the frequencies of positive and negative emotions observed in emails. The figures show the number of cases.

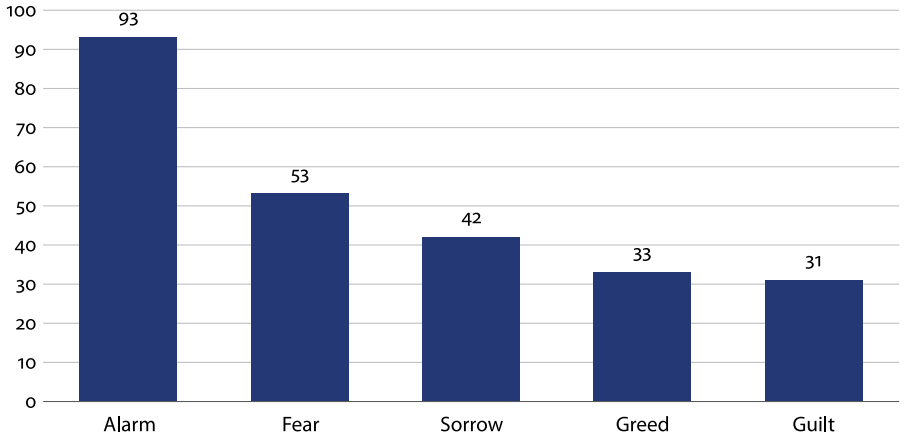

Figure 1. Raw counts of negative emotions identified in scam emails

One of the most striking features of Figure 1 is the high frequency of negative emotions such as fear, alarm, and anxiety. This prevalence underscores the effectiveness of these emotions in coercing recipients into making hasty decisions. The dominance of negative emotional triggers can be surprising and highlights the tactics that scammers use to exploit vulnerabilities.

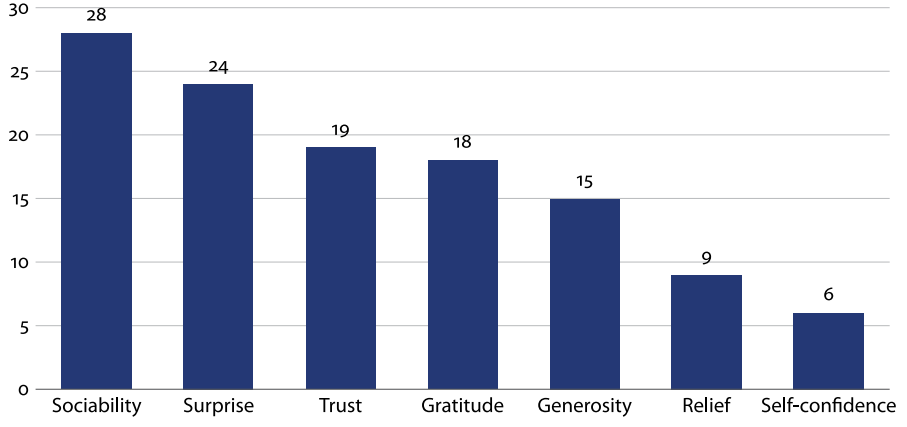

Figure 2. Raw counts of positive emotions recognized in scam emails

The presence of positive emotions such as sociability, trust, and gratitude in scam emails indicates that scammers do not rely solely on negative emotions to manipulate victims; they also attempt to create a false sense of connection and trust. This dual approach is intriguing because it reveals the complexity of emotional manipulation in deceptive communication. By highlighting the positive

emotions, Figure 2 can help victims understand how scammers exploit recipients' altruistic tendencies and desire for social connections. When viewed alongside Figure 1, the contrast between the frequencies of negative and positive emotions is compelling. This juxtaposition emphasizes the strategic focus of scammers on inducing fear and urgency while also revealing that they occasionally employ positive emotions to build trust.

4.2 Combinations of emotional triggers

Scam emails often employ various combinations of emotional triggers to manipulate recipients. While specific combinations can vary, Table 4 reveals common emotional triggers observed in the dataset:

Table 4. Combinations of emotional triggers in scam emails

Combinations	Elaboration	Sample message content	Frequency	Percentage
Alarm + Fear	Scammers create a sense of urgency and fear by claiming that immediate action is required to avoid negative consequences, such as account suspension, legal trouble, and financial loss.	Your account has been compromised. Take immediate action to prevent unauthorized access and potential financial loss.	45	43%
Greed + Alarm	Scammers appeal to individuals' desire for financial gain by offering limited-time or exclusive deals. They create a sense of scarcity that makes recipients feel that they must act quickly to secure the promised benefits.	Only 10 spots left to invest in this exclusive opportunity that guarantees high returns.	29	28%
Guilt + Sociability	Scammers may exploit individuals' sense of guilt by claiming to represent a charitable cause or a person in need. They appeal to recipients' sociability by emphasizing the importance of helping others and making them feel responsible for taking action.	Your donation will make a difference in the lives of children suffering from this devastating disease. Act now and be part of this important cause.	11	10%

Table 4. *(continued)*

Combinations	Elaboration	Sample message content	Frequency	Percentage
Surprise + Trust	Scammers may use unexpected or surprising information to attract recipients' attention. They also try to establish trust by impersonating a reputable organization or using familiar logos, making it more likely for individuals to believe the content of an email.	Congratulations! You've won a free vacation! Claim your prize by providing your personal details within 24 hours.	10	10%
Gratitude + Generosity	Scammers may offer something of perceived value, such as a free gift or a chance to win a prize. They may also appeal to recipients' altruistic nature by claiming that their actions will benefit a charitable cause or help others in need.	Donate $ 50 and receive a free gift worth $ 100! Your contribution will support underprivileged children and provide them with essential resources.	5	5%
Relief + Self-confidence	Scammers may exploit individuals' desire to escape a problem or difficult situation. They offer solutions or opportunities that promise to alleviate stress or improve personal circumstances, boosting recipients' self-confidence in making a positive change.	Our proven system will help you earn a six-figure income from the comfort of your home. Take control of your financial future today.	4	4%

The combination of *alarm* and *fear* is a common tactic used by scammers to create a sense of urgency and pressure recipients to take immediate action. By claiming that negative consequences, such as account suspension, legal trouble, or financial loss, would occur if they do not act quickly, scammers aim to instill fear and panic in recipients. This combination was observed in 45 instances, indicating its prevalence in attempting to capture the attention and of victims. In addition, the combination of *greed* with *alarm* was observed in 29 instances. By appealing to individuals' desire for financial gains and offering limited-time

opportunities or exclusive deals, scammers create a feeling that the demand for a good or service is greater than the availability of the good or service. They make recipients believe that they must act quickly to secure the promised benefits.

Scammers also exploit individuals' sense of *guilt* and *sociability* to represent a charitable cause or a person in need by appealing to recipients' empathy and responsibility to help others. This combination was observed in 11 cases, demonstrating the scammers' efforts to manipulate recipients' emotions and make them feel obligated to take action. The combination of *surprise* and *trust* is used by scammers to capture recipients' attention and establish credibility. By providing unexpected or surprising information and impersonating reputable organizations or using familiar logos, scammers make recipients more susceptible to the content of the email. This combination was observed in 10 cases, demonstrating that scammers attempt to exploit recipients' curiosity and trust. Scammers may also combine *gratitude* and *generosity* to manipulate recipients. By offering a token of perceived value, such as a free gift or a chance to win a prize, and appealing to recipients' altruistic nature by claiming that their actions will benefit a charitable cause or help others in need, scammers aim to elicit a response. This combination was observed in 5 instances, indicating that scammers attempt to tap into recipients' generosity and desire to make a positive impact. Finally, *relief* combined with *self-confidence* is another tactic employed by scammers. By exploiting individuals' desire for relief from a problem or difficult situation and offering solutions or opportunities that promise to alleviate stress or improve personal circumstances, scammers aim to boost recipients' self-confidence in making a positive change. This combination was observed in 4 instances, emphasizing scammers' attempts to manipulate recipients' emotions and persuade them to take action.

4.3 Qualitative analysis of scam emails

The qualitative analysis of scam emails involves examining the content, structure, and emotional triggers used by scammers to manipulate recipients. This analysis provides insights into the psychological tactics employed and their effectiveness in eliciting responses from potential victims. Although these emails are scam emails, proper names referring to places and people mentioned in these emails may resemble real names and real identities. Thus, proper names were removed from the emails to maintain anonymity. In addition, the grammatical and syntactic errors present in the scam emails were not corrected during the analysis process to maintain the authenticity of the emails.

Email 1 Greetings
My name is Miss .... It give me a great pleasure to write you, it attracts me to write to you so that we can be friends if you will have the desire as me. i will be very happy to be in communication with you so that we can get to know each other better and see what happens in future. I await your reply so that i can tell you more about myself and give you my picture.
Have a blessed day.
Miss ...

Email (1) expresses a desire for friendship and communication that appeals to the recipient's sociability. The sender's intention to connect and get to know the recipient better is a clear attempt to establish a personal connection, making the recipient more inclined to trust the sender. The friendly tone and the offer to share more personal information (such as a picture) are strategies to build trust. The sender attempts to create a sense of familiarity that can lower the recipient's defense and make them more receptive to further communication.

Email 2 Dear Friend,
I Mr ..., Manager of bill and exchange at ... BANK in Burkina Faso, I would like you to indicate your interest to receive the transfer of (12.3 Million Dollars) in your bank account, I will like you to stand as the next of kin to a deceased customer who die in plane crash.
Thanks for your co-operation.
Your Sincerely,
Mr ...

In Email (2), the promise of receiving a large sum of money ($ 12.3 million) appeals to the recipient's greed. This emotional trigger is powerful because it can cause individuals to overlook potential red flags in emails due to the allure of financial gain. The sender identifies himself as a bank manager to establish credibility and trust. By presenting himself in a position of authority, the sender makes the recipient feel secure about the legitimacy of the offer, despite the inherent risks. The email referenced a deceased customer who died in a plane crash. This mention inherently carries the connotation of loss and tragedy, which can evoke feelings of sorrow in the recipient. The sender may leverage this emotional aspect to create a narrative that elicits sympathy, making the recipient more inclined to respond favorably to the request.

Email 3 Greetings,
We noticed that you did not log into your ESL account for nearly 4 years and we are writing to inform you that we will unfortunately have to close your account soon. We are forced to do this due to our GDPR policy that prevents us from keeping user data for more than 4 years.

Kindly send me the following information to keep your account active:
Full Names
Address
Occupation
Direct Mobile Telephone Lines
Nationality
Thank you for being a valued member of our ESL family! We appreciate your attention to this matter and look forward to hearing from you soon.
Your team

In Email (3), the urgency implied in the statement about the impending account closure serves as an alarm. The mention of a specific timeframe (nearly 4 years) and the need for immediate action to prevent account closures can heighten a recipient's sense of urgency, prompting them to act quickly. In addition, expressing appreciation for the recipient's attention and their status as a community member can evoke feelings of gratitude, encouraging them to respond positively.

Email 4 Dear Friend,
Greetings!
How are you with your family today? I hope both of you are in good health. Decently I know that this message might meet you in utmost surprise as both of us never know each other before. I am Mr [name blocked]; a banker by profession, I need your urgent assistance in transferring the sum of $ 21.7 Million U.S Dollars into your account. It is 100% risk free and under this achievement you are entitled to receive 30% of the total cash. More details will be sent to you on confirmation of your interest.
If this money remains unclaimed after my death, the bank executives or the government will take the money as unclaimed fund and maybe use it for selfish and worthless ventures, I need a very honest person who can claim this money and use it for Charity works, for orphanages, widows and also build schools for less privilege that will be named after my late husband and my name.
Regards
Mr. …

In Email (4), the email introduces a sense of fear by stating that if the money remains unclaimed after the sender's death, it will be taken by the bank or government for 'selfish and worthless ventures.' This tactic instills fear of loss and urgency by compelling the recipient to act quickly to avoid a negative outcome. The phrase '100% risk free' is designed to address any concerns that the recipient may have regarding the legitimacy of the transaction. This reassurance can create a sense of comfort and encourage the recipient to consider the offer more seriously. Framing the potential use of funds as selfish and worthless evokes feelings

of guilt in the recipient. The implication is that failing to act can result in a missed opportunity, which can pressure the recipient into compliance.

The qualitative analysis of scam emails revealed sophisticated strategies employed by scammers to exploit emotional triggers and manipulate recipients. By combining elements of urgency, financial incentives, and emotional appeals, scammers create compelling narratives that can easily deceive individuals. Understanding these tactics is crucial for developing effective preventive measures and raising awareness about the risks associated with such communication. Recognizing the emotional and structural components of scam emails can empower individuals to critically evaluate suspicious messages and protect themselves from potential fraud.

5. Discussion

By systematically analyzing a set of scam emails collected over five years, this study provides a detailed account of how negative and positive emotions can be employed as tools of manipulation. The distinguishing feature of the study is the depth of analysis it provides regarding the emotional dynamics at play. While prior research has acknowledged the role of negative emotions (Shadel and Pak 2007; Goldenberg and Gross 2020), our employed Robinson's (2008) emotional taxonomy to identify a diverse range of positive and negative emotions scammers use to influence behavior. This nuanced understanding of emotional patterns enriches the theoretical framework related to emotional manipulation in digital communication, providing deeper insights into the mechanisms that lead individuals to fall victim to scams.

To answer the first research question, we coded emotions evoked in scam emails into negative and positive categories to understand the psychological strategies used by scammers to elicit specific responses from recipients. A key finding in this study was that negative emotional triggers such as 'alarm' and 'fear' were frequently used in scam emails. Such negative emotions likely create a sense of immediate action and reduce the recipient's ability to think critically or question the legitimacy of the email. While both 'fear' and 'alarm' are negative emotions that scammers exploit, *fear* is more about the underlying threat and emotional distress, whereas *alarm* is about the urgency and immediate need to act in response to that threat. Scammers use both emotions strategically to manipulate recipients into making hasty decisions, but they do so through different emotional appeals. This highlights the effectiveness of negative emotions in capturing victims' attention and coercing them into taking action. The use of alarm and fear tactics, such as emphasizing the need for immediate attention or warning of dire

consequences, aims to foster a sense of vulnerability and pressure recipients to respond quickly. In this regard, our findings lend support to those of Shadel and Pak (2007) who found fear and intimidation accounted for 45.24% of all tactics used. This is also in line with other studies that showed how scammers exploit urgency and fear to compel recipients to act quickly, often without critical evaluation (Carter 2015). The contribution of the present study is that it demonstrates how these emotions were embedded in scam emails through a systematic analysis of emotions.

The prevalence of negative emotions in our data deserves some discussion. According to Robinson (2008), negative emotions are powerful emotional states that can significantly influence human behavior, often compelling individuals to act in ways they might not otherwise consider. These emotions can serve as strong motivators, driving people to respond to perceived threats or uncertainties in their environment. By threatening negative outcomes if demanded actions are not taken, scammers manipulate individuals to respond impulsively. For example, echoing Chiluwa's (2019) findings, some of the negative emotions identified in the present study appealed to death or religious sentiments. Consistent with prior research that emphasized how the potential loss of a reward or monetary gain can influence victims' compliance with phishing requests (Vishwanath, Harrison and Ng 2018), our findings showed similar patterns in scam emails where monetary gains manifest as feelings of relief or comfort when responding to a request.

Although negative emotions such as *fear* and *urgency* are prominently utilized by scammers to manipulate recipients, the presence of positive emotions in scam emails cannot be overlooked. Among these, 'sociability' emerges as the most dominant positive emotional trigger. Scammers often craft messages that evoke a sense of connection and trust, appealing to recipients' altruistic tendencies and desire for social interaction. By appealing to sociability, surprise, trust, gratitude, and generosity, scammers aim to create a false sense of camaraderie, gratitude, or obligation in recipients, making them more susceptible to the scam. As argued by Freiermuth (2011), scammers' main goal is to engage victims and create solidarity, and the best way to do so is by building trust. Freiermuth (2011: 123) further states that "scammers are most concerned about building solidarity with the mark [victim] and playing to a mark's egocentrism, both of which keep the mark from making well-informed decisions." By understanding how scammers exploit positive and negative emotions, we gain valuable insights into their psychological strategies. This knowledge is essential for developing effective countermeasures and enhancing public awareness, which empowers individuals to recognize and resist the multifaceted tactics employed in online scams.

In response to our second research question, the findings of this study demonstrate that scammers also take advantage of a combination of emotions in their e-

messages. Carter (2015: 99) discusses that "trust, credibility, urgency and secrecy are key facets of scam mail." By exploiting a range of positive and negative combinations of emotional triggers, scammers can manipulate individuals' decision-making processes, leading them to act against rational judgment. This dual approach — leveraging both negative and positive emotions — highlights the complexity of emotional manipulation in deceptive communication.

The findings of this research indicate that the occurrence of a promise for a reward is less frequent than that of a loss, which indicates that the negative implications of scarcity might manipulate users more than potential gains. As discussed earlier in the Introduction, negative emotions play a much more central role in digital communication, as evidenced by the massive circulation of negative content (Hornik et al. 2015; Goldenberg and Gross 2020). Consequently, it is not unusual that scam emails exhibit a similar pattern, as negative emotions are particularly effective in capturing immediate attention and prompting compliance. This finding aligns with the psychological principle that negative stimuli often elicit stronger responses than positive stimuli. For instance, a scam email that warns recipients of potential account suspension or legal repercussions creates a sense of urgency that compels individuals to act quickly, often without fully assessing the situation. In contrast, while positive emotions can also be employed — such as promises of financial gains or rewards — they are less frequently observed in scam communications. For example, an email stating, 'Congratulations! You've won a prize!' may elicit excitement, but it often lacks the immediate urgency that negative emotions trigger.

This study underscores the diverse range of emotional triggers that play a pivotal role in shaping the driving force behind scam emails (Serna-Zuluaga et al. 2024). Scammers often exploit a range of emotional triggers — such as fear, urgency, sociability, trust, and greed — to manipulate individuals into making hasty decisions that they might not otherwise consider (Robinson 2008). According to Blunden and Brodsky (2021: 10), "email and other text-based communications have a significantly greater variety of emotional cues than historical theories of virtual communication propose." This underscores the necessity for a nuanced understanding of how emotional appeals function within the context of digital communication. By recognizing the specific emotional triggers employed by scammers, individuals can develop heightened awareness and critical thinking skills that enable them to resist manipulation. In addition, this study highlights the importance of integrating emotional literacy into cybersecurity education, to equip users with tools to identify and respond to potential threats effectively. Ultimately, fostering an informed and emotionally aware online community can serve as a formidable defense against the pervasive issue of scam emails, promoting safer digital interactions, and reducing the likelihood of victimization.

6. Implications and conclusions

The implications of this study for discourse pragmatics are significant, particularly for understanding how emotional manipulation shapes communicative interactions in digital contexts. The findings reveal that scammers effectively leverage both positive and negative emotions to influence recipient behavior, highlighting the necessity for discourse pragmatics to incorporate emotional analysis as a core component of its framework. By recognizing that emotional triggers are not merely supplementary to the content of communication but are integral to its pragmatic function, researchers can gain deeper insights into how language operates in persuasive and deceptive contexts. This study indicates that the emotional landscape of discourse — encompassing feelings of urgency, trust, and sociability — plays a crucial role in shaping the interpretive processes of recipients (Levy 2016).

The findings of this study have broader implications for corporate and business communication, public awareness and education. By highlighting the emotional tactics used by scammers, we highlight the critical need for targeted educational initiatives that focus on these manipulative strategies. Specifically, awareness-raising programs should aim to teach individuals how to identify common emotional triggers in scam communications, such as fear, urgency, and false promises of reward. For instance, workshops or online courses could provide practical examples of scam emails, illustrating how emotional manipulation can be employed to elicit impulsive responses. Participants could engage in exercises that train them to recognize red flags, such as language that creates a sense of panic or urgency, and to adopt a more skeptical approach when encountering unsolicited messages (also see Fransen, Smit and Verlegh 2015). Additionally, educational materials could include guidelines on how to verify the legitimacy of requests for personal information or financial transactions, emphasizing the importance of taking time to assess the situation rather than reacting immediately. By equipping individuals with these skills, we can foster a more awareness to resist emotional manipulation and protect themselves from becoming victims of scams. This proactive approach not only enhances individual resilience but also contributes to broader efforts to promote online safety and security as well as our understanding of discourse pragmatics in the age of online interactions.

Further exploration of the psychological mechanisms that lead individuals to comply with scam requests despite their awareness of potential risks can provide valuable insights. Emotional strategies used in other forms of scams, such as romance and employment scams, may differ significantly. Future research should consider a broader range of scam types to capture the full spectrum of emotional manipulation techniques. As scams occur more frequently through

social media platforms, research should focus on how emotional manipulation tactics are adapted for these environments. Moreover, this study mainly used the emotional taxonomy proposed by Robinson (2008). Using more up-to-date taxonomies yields interesting results. This could involve studying factors such as personality traits, cognitive biases, and situational contexts that influence decision-making despite emotional appeals. In addition, future research can investigate qualitatively the experiences and insights of recipients who fell victim to scam emails. Understanding what specifically led them to comply with the scammers' requests could offer deeper insights into the effectiveness of these tactics. This could also shed light on how emotional triggers interact with individual psychological factors, such as personality traits, cognitive biases, or situational pressures. Incorporating these perspectives could complement the current focus on emotional taxonomy and provide a more holistic understanding of the mechanisms driving compliance in scam scenarios.

Funding

Open Access publication of this article was funded through a Transformative Agreement with University of Reading.

References

Ajayi, Temitope Michael. 2022. "Discursive-manipulative strategies in scam emails and SMS: The Nigerian perspective." *Lodz Papers in Pragmatics* 18(1): 175–195.

Aleroud, Ahmed, and Lina Zhou. 2017. "Phishing environments, techniques, and countermeasures: A survey." *Computers & Security* 68: 160–196.

Alkhalil, Zainab, Chaminda Hewage, Liqaa Nawaf, and Imtiaz Khan. 2021. "Phishing attacks: A recent comprehensive study and a new anatomy." *Frontiers in Computer Science* 3, 563060.

Almomani, Ammar, Brij B. Gupta, Samer Atawneh, Andrew Meulenberg, and Eman Almomani. 2013. "A survey of phishing email filtering techniques." *IEEE Communications Surveys & Tutorials* 15(4): 2070–2090.

Anafo, Comfort, and Richmond S. Ngula. 2020. "On the grammar of scam: transitivity, manipulation and deception in scam emails." *Word* 66(1): 16–39.

Bernal, Miriam Jiménez, and Simone Belli. 2013. "Virtual ethnography and spam: Fraud and fear in deceptive narratives on the Internet." In *Investigar la Comunicación hoy. Revisión de políticas científicas y aportaciones metodológicas: Simposio Internacional sobre Política Científica en Comunicación* [*International Symposium on Scientific Policy in Communication: Examining Current Research, Policy Reviews, and Methodological Advances*], 205–217. Facultad de Ciencias Sociales, Juridicas y de la Comunicación.

Blanzieri, Enrico, and Anton Bryl. 2008. "A survey of learning-based techniques of email spam filtering." *Artificial Intelligence Review* 29(1): 63–92.

Blommaert, Jan, and Tope Omoniyi. 2006. "Email fraud: Language, technology, and the indexicals of globalisation." *Social Semiotics* 16(4): 573–605.

Blunden, Hayley, and Andrew Brodsky. 2021. "Beyond the emoticon: Are there unintentional cues of emotion in email?" *Personality and Social Psychology Bulletin* 47(4): 565–579.

Bourne, Paul Andrew, Chad Chambers, Damion K. Blake, Charlene Sharpe-Pryce, and Ikhalfani Solan. 2013. "Lottery scam in a third-world nation: the economics of a financial crime and its breadth." *Asian Journal of Business Management* 5(1): 19–51.

Carter, Elisabeth. 2015. "The anatomy of written scam communications: An empirical analysis." *Crime, Media, Culture* 11(2): 89–103.

Chawki, Mohamed. 2009. "Nigeria tackles advance fee fraud." *Journal of information, Law and Technology* 1(1): 1–20.

Chiluwa, Innocent. 2009. "The discourse of digital deceptions and '419' emails." *Discourse Studies* 11(6): 635–660.

Chiluwa, Innocent. 2019. "'Congratulations, your email account has won you €1,000,000': analyzing the discourse structures of scam emails." In *The Palgrave Handbook of Deceptive Communication*, ed. by Tony Docan-Morgan, 897–912. Cham: Palgrave Macmillan.

Cukier, Wendy L., Eva J. Nesselroth, and Susan Cody. 2007. "Genre, narrative and the 'Nigerian Letter' in electronic mail." Paper presented at 40th Annual Hawaii International Conference on System Sciences (HICSS'07). Waikoloa, HI, USA, 3–6 January 2007.

Daintith, John, and Edmund Wright (eds.). 2008. *A Dictionary of Computing* (6th edn.). Oxford: Oxford University Press.

Dirwan, Dirwan, and Fitriani Latief. 2023. "Understanding the psychology behind consumer behavior." *Advances in Business & Industrial Marketing Research* 1(3): 130–145.

Dutt, Bindiya. 2023. "Wellbeing amid digital risks: implications of digital risks, threats, and scams on users' wellbeing." *Media and Communication* 11(2): 355–366.

Febriyani, Widia, Dhiya Fathia, Adityas Widjajarto, and Muharman Lubis. 2023. "Security awareness strategy for phishing email scams: A case study of a company in Singapore." *JOIV: International Journal on Informatics Visualization* 7(3): 808–814.

Fischer, Peter, Eva Jonas, Dieter Frey, and Stefan Schulz-Hardt. 2005. "Selective exposure to information: The impact of information limits." *European Journal of Social Psychology* 35(4): 469–492.

Fransen, Marieke L., Edith G. Smit, and Peeter W. J. Verlegh. 2015. "Strategies and motives for resistance to persuasion: An integrative framework." *Frontiers in Psychology* 6, 1201.

Fredericks, Paul, and Matthew Rowe. 2016. "Charity fraud." In *Fraud*, ed. by Alan Doig, 215–233. New York: Routledge.

Freiermuth, Mark R. 2011. "Text, lies and electronic bait: An analysis of email fraud and the decisions of the unsuspecting." *Discourse & Communication* 5(2): 123–145.

Genc, Yegin, Harpreet Kour, Hasan T. Arslan, and Li-Chiou Chen. 2021. "Understanding Nigerian e-mail scams: A computational content analysis approach." *Information Security Journal: A Global Perspective* 30(2): 88–99.

Goldenberg, Amit, and James J. Gross. 2020. "Digital emotion contagion." *Trends in Cognitive Sciences* 24(4): 316–328.

Hatfield, Elaine, John T. Cacioppo, and Richard L. Rapson. 1993. "Emotional contagion." *Current Directions in Psychological Science* 2(3): 96–100.

Holt, Thomas J., and Danielle C. Graves. 2007. "A qualitative analysis of advance fee fraud e-mail schemes." *International Journal of Cyber Criminology* 1(1): 137–154.

Hornik, Jacob, Rinat Shaanan Satchi, Ludovica Cesareo, and Alberto Pastore. 2015. "Information dissemination via electronic word-of-mouth: Good news travels fast, bad news travels faster!" *Computers in Human Behavior* 45: 273–280.

Jayatilaka, Asangi, Nalin Asanka Gamagedara Arachchilage, and Muhammad Ali Babar. 2021. "Falling for phishing: An empirical investigation into people's email response behaviors." Paper presented at the 42nd International Conference on Information Systems (ICIS'21). Austin, Texas, USA, 12–15 December 2021. https://arxiv.org/pdf/2108.04766v1

Jonas, Eva, Verena Graupmann, and Dieter Frey. 2006. "The influence of mood on the search for supporting versus conflicting information: Dissonance reduction as a means of mood regulation?" *Personality and Social Psychology Bulletin* 32(1): 3–15.

Karamagi, Robert. 2022. "A review of factors affecting the effectiveness of phishing." *Computer and Information Science* 15(1): 1–32.

Karim, Asif, Sami Azam, Bharanidharan Shanmugam, Krishnan Kannoorpatti, and Mamoun Alazab. 2019. "A comprehensive survey for intelligent spam email detection." *IEEE Access* 7: 168261–168295.

Keil, Mark, and Roy D. Johnson. 2002. "Feedback channels: Using social presence theory to compare voice mail to e-mail." *Journal of Information Systems Education* 13(4): 295–303.

Kensinger, Elizabeth A., and Jaclyn H. Ford. 2020. "Retrieval of emotional events from memory." *Annual Review of Psychology* 71(1): 251–272.

Khan, Wazir Zada, Muhammad Khurram Khan, Fahad T. Bin Muhaya, Mohammed Y. Aalsalem, and Han-Chieh Chao. 2015. "A comprehensive study of email spam botnet detection." *IEEE Communications Surveys & Tutorials* 17(4): 2271–2295.

Korpela, Karina. 2015. "Improving cyber security awareness and training programs with data analytics." *Information Security Journal: A Global Perspective* 24(1–3): 72–77.

Kwak, Youngsun, Seyoung Lee, Amanda Damiano, and Arun Vishwanath. 2020. "Why do users not report spear phishing emails?" *Telematics and Informatics* 48: 101343.

Lerner, Jennifer S., Ye Li, Piercarlo Valdesolo, and Karim S. Kassam. 2015. "Emotion and decision making." *Annual Review of Psychology* 66(1): 799–823.

Levy, Nadine. 2016. "Emotional landscapes; discomfort in the field." *Qualitative Research Journal* 16(1): 39–50.

Metzger, Miriam J., Andrew J. Flanagin, and Ryan B. Medders. 2010. "Social and heuristic approaches to credibility evaluation online." *Journal of Communication* 60(3): 413–439.

Morris, Michael W., and Dacher Keltner. 2000. "How emotions work: The social functions of emotional expression in negotiations." *Research in Organizational Behavior* 22: 1–50.

Nadeem, Muhammad, Syeda Wajiha Zahra, Muhammad Nouman Abbasi, Ali Arshad, Saman Riaz, and Waqas Ahmed. 2023. "Phishing attack, its detections and prevention techniques." *International Journal of Wireless Security and Networks* 1(2): 13–25.

Naqvi, Bilal, Kseniia Perova, Ali Farooq, Imran Makhdoom, Shola Oyedeji, and Jari Porras. 2023. "Mitigation strategies against the phishing attacks: A systematic literature review." *Computers & Security* 132, 103387.

Naylor, R. Thomas. 2007. "The alchemy of fraud: Investment scams in the precious-metals mining business." *Crime, Law and Social Change* 47: 89–120.

Norris, Gareth, and Alexandra Brookes. 2021. "Personality, emotion, and individual differences in response to online fraud." *Personality and Individual Differences* 169, 109847.

Parsons, Kathryn, Marcus Butavicius, Paul Delfabbro, and Meredith Lillie. 2019. "Predicting susceptibility to social influence in phishing emails." *International Journal of Human-Computer Studies* 128: 17–26.

Pellegrino, Alfonso, Masato Abe, and Randall Shannon. 2022. "The dark side of social media: Content effects on the relationship between materialism and consumption behaviors." *Frontiers in Psychology* 13, 870614.

Robinson, David L. 2008. "Brain function, emotional experience and personality." *Netherlands Journal of Psychology* 64: 152–168.

Safaei Pour, Morteza, Christelle Nader, Kurt Friday, and Elias Bou-Harb. 2023. "A comprehensive survey of recent internet measurement techniques for cyber security." *Computers & Security* 128, 103123.

Safi, Asadullah, and Satwinder Singh. 2023. "A systematic literature review on phishing website detection techniques." *Journal of King Saud University Computer and Information Sciences* 35(2): 590–611.

Serna-Zuluaga, Juan Camilo, David Juárez-Varón, Ana Mengual-Recuerda, and Ana Medina-López. 2024. "Analysis of the influence of emotions on the decision-making of entrepreneurs using neurotechnologies." *International Entrepreneurship and Management Journal* 20: 2169–2186.

Shadel, Doug, and Karla Blair Schweitzer Pak. 2007. "The psychology of consumer fraud." PhD dissertation, Universiteit van Tilburg.

Shaw, Philip. 2008. "Purpose and other paradigmatic similarities as criteria for genre analysis: The case of '419 scam' emails." In *Genre Variation in Business Letters*, ed. by Paul Gillaerts, and Maurizio Gotti, 257–280. Bern: Peter Lang.

Shichor, David, Jeffrey Doocy, and Gilbert Geis. 1996. "Anger, disappointment, and disgust: Reactions of victims of a telephone investment scam." In *International Victimology: Selected Papers From the 8th International Symposium*, ed. by Chris Sumner, Mark Israel, Michael O'Connell, and Rick Sarre, 105–112. Canberra: Australian Institute of Criminology.

Silic, Mario, and Andrea Back. 2016. "The dark side of social networking sites: Understanding phishing risks." *Computers in Human Behavior* 60: 35–43.

Sillence, Elizabeth, Pam Briggs, Peter Harris, and Lesley Fishwick. 2006. "A framework for understanding trust factors in web-based health advice." *International Journal of Human-Computer Studies* 64(8): 697–713.

Sorell, Tom, and Monica Whitty. 2019. "Online romance scams and victimhood." *Security Journal* 32: 342–361.

Stojnic, Tatyana, Dinusha Vatsalan, and Nalin A. G. Arachchilage. 2021. "Phishing email strategies: Understanding cybercriminals' strategies of crafting phishing emails." *Security and Privacy* 4(5), e165.

Tambe Ebot, Alain Claude, Mikko Siponen, and Volkan Topalli. 2024. "Towards a cybercontextual transmission model for online scamming." *European Journal of Information Systems* 33(4): 571–596.

Tseng, Ming-Yu. 2010. "The pragmatic act of fishing for personal details: From choice to performance." *Journal of Pragmatics* 42(7): 1982–1996.

Vilardo, Mark F. 2004. "Online impersonation in securities scams." *IEEE Security & Privacy* 2(3): 82–85.

Vishwanath, Arun, Brynne Harrison, and Yu Jie Ng. 2018. "Suspicion, cognition, and automaticity model of phishing susceptibility." *Communication Research* 45(8): 1146–1166.

Vishwanath, Arun, Tejaswini Herath, Rui Chen, Jingguo Wang, and H. Raghav Rao. 2011. "Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model." *Decision Support Systems* 51(3): 576–586.

Wash, Rick. 2020. "How experts detect phishing scam emails." *Proceedings of the ACM on Human-Computer Interaction* 4(CSCW2): 1–28.

Wiles, Rose, Graham Crow, Sue Heath, and Vikki Charles. 2008. "The management of confidentiality and anonymity in social research." *International Journal of Social Research Methodology* 11(5): 417–428.

Workman, Michael. 2008. "Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security." *Journal of the American Society for Information Science and Technology* 59(4): 662–674.

Zhou, Lina, Douglas P. Twitchell, Tiantian Qin, Judee K. Burgoon, and Jay F. Nunamaker. 2003. "An exploratory study into deception detection in text-based computer-mediated communication." In *Proceedings of the Thirty-Sixth Hawaii International Conference on System Sciences*, 1–10. Los Alamitos, CA: IEEE Press.

Address for correspondence

Erhan Aslan
University of Reading
Edith Morley Building
Office 210B Shinfield Road
Whiteknights
Reading Berkshire RG6 6EL
UK

erhan.aslan@reading.ac.uk

Biographical notes

Mostafa Morady Moghaddam is an Associate Professor at Shahrood University of Technology, Shahrood, Iran. His research projects mainly focus on social psychology. Mostafa studies social influence, perception, and interaction in various settings, including institutional discourse and classroom dynamics. He has published his research outputs in *Foreign Language Annals*,

Lingua, *Pragmatics*, *Pragmatics and Cognition*, *Language Teaching Research*, and *Asia-Pacific Education Researcher*, among others. His monograph on "indirect reports" was published by Springer in 2019.

Erhan Aslan is Associate Professor of Applied Linguistics at the University of Reading. He received his Ph.D. in Second Language Acquisition and Instructional Technology from the University of South Florida. His current research interests include language in the digital media, particularly internet memes and online metacommentary. His work appeared in journals, such as the *Journal of Sociolinguistics*, the *Journal of Pragmatics*, and the *CALICO Journal*. He is also one of the co-authors of "Language and Media" (2nd edition) published by Routledge (2020).

Publication history

Date received: 4 May 2025
Date accepted: 7 January 2026
Published online: 4 March 2026