Open Access License Notice

Persuasion and Phishing: Analysing the Interplay of Persuasion Tactics in Cyber Threats

Kalam Khadka
Faculty of Science and Technology
University of Canberra
Canberra, Australia
0000-0003-2567-9585

Abstract—This study extends the research of Ferreira and Teles (2019), who synthesized works by Cialdini (2007), Gragg (2003), and Stajano and Wilson (2011) to propose a unique list of persuasion principles in social engineering. While Ferreira and Teles focused on email subject lines, this research analyzed entire email contents to identify principles of human persuasion in phishing emails. This study also examined the goals and targets of phishing emails, providing a novel contribution to the field. Applying these findings to the ontological model by Mouton et al. (2014) reveals that when social engineers use email for phishing, individuals are the primary targets. The goals are typically unauthorized access, followed by financial gain and service disruption, with 'Distraction' as the most commonly used compliance principle. This research highlights the importance of understanding human persuasion in technology-mediated interactions to develop methods for detecting and preventing phishing emails before they reach users. Despite previous identification of luring elements in phishing emails, empirical findings have been inconsistent. For example, Akbar (2014) found 'Authority' and 'Scarcity' most common, while Ferreira et al. (2015) identified 'Liking and Similarity.' In this study, 'Distraction' was most frequently used, followed by 'Deception,' 'Integrity,' and 'Authority.' This paper offers additional insights into phishing email tactics and suggests future solutions should leverage socio-technical principles. Future work will apply this methodology to other social engineering techniques beyond phishing emails, using the ontological model to further inform the research community.

Keywords—*Phishing, Social Engineering, Persuasion, Ontological Model*

I. INTRODUCTION

Phishing is a form of cybercrime that involves impersonating a trustworthy entity to trick users into disclosing sensitive information or performing malicious actions [1]. Phishing involves using a blend of social engineering tactics and technical strategies to persuade individuals to disclose their personal information [2]. Social engineering attacks, particularly phishing, pose significant cybersecurity threats by exploiting human vulnerabilities to obtain sensitive information [2] [3]. Social engineering exploits human vulnerabilities using persuasion principles to gather information and conduct cyber-attacks [4]. Moreover, Phishing emails using social engineering techniques are effective at exploiting human vulnerabilities [5]. Human vulnerabilities pose significant challenges in cybersecurity, with studies indicating that 95% of successful cyber-attacks result from human error [6]. Contextualizing phishing emails to appeal to psychological weaknesses increases susceptibility to deception and vulnerability to phishing [7]. Humans are the weakest link in cybersecurity due to vulnerabilities exploited by social engineering tactics [8]. Integrating human factors with technical solutions can enhance cybersecurity by addressing user vulnerabilities and improving security culture [9]. Phishing, particularly through email delivery, remains a prevalent and costly method of cyberattack. According to the ACC (2024) report, phishing scams have resulted in financial losses amounting to $5,437,833 in Australia from Jan. to May 2024, the total amount lost to various scams including phishing, reached $113,270,400, reflecting the substantial economic impact of these cyber threats. Despite comprising only 7% of all scam reports, these phishing attempts have demonstrated a high effectiveness in extracting financial information from victims [10]. The persistent use of phishing emails demonstrates their potency in deceiving individuals by mimicking legitimate communications to harvest sensitive information and execute financial fraud.

Phishing emails are successful because they leverage social engineering techniques, exploiting human psychology and social interactions [5] [11]. They appear credible by using personal and contextual details about their targets, effectively persuading victims to disclose sensitive information and transfer money [12]. The author suggests that phishing emails often incorporate various persuasion principles and techniques to enhance their effectiveness. Therefore, analysing and identifying these principles and behavioural traits in emails can potentially improve and support existing phishing detection tools and making aware about the cyber security threats.

Persuasion, commonly associated with marketing and sales, is a powerful tool that can be applied to any human interaction, including cyber-attacks. It is often used to create convincing phishing emails [1] [11]. Cialdini (2007), Gragg

(2003), and Stajano and Wilson (2011) have outlined various persuasion principles frequently employed by humans. Ferreira and Teles (2019) have integrated the three perspectives to derive a unique, complete, and systematized list of principles.

Phishing emails employ various persuasion techniques to deceive recipients. Analysing the content and persuasive elements of phishing emails can provide insights into how they are designed to be persuasive [13] [14]. Phishers often use email to launch their attacks, relying on persuasion to trick unsuspecting victims into responding positively. To protect users, it's crucial for system designers and security professionals to understand how these persuasive techniques work in phishing emails. This study analyses these techniques to better understand how phishing emails operate in the real world.

This study builds upon Ferreira & Teles' (2019) foundational research, which synthesized key Principles of Persuasion from the works of Cialdini (2007), Gragg (2003), and Stajano and Wilson (2011). Using a coding framework derived deductively from these integrated principles, the current research conducted content analysis on a random selection of 200 phishing emails. These emails were sourced from millersmiles.co.uk, a reputable international repository of reported spoof emails and phishing scams spanning from 2014 to 2023.

II. PRINCIPLES OF PERSUASION

Persuasion is the art of effective speaking and writing to influence the audience through logic, emotion, and credibility, it is also a goal-oriented use of language aimed at influencing attitudes and behaviours [15]. The principle of persuasion has been a subject of research for decades, with various studies exploring its mechanisms and applications. Early studies focused on identifying factors influencing message processing in persuasive communications [16]. Information systems researchers have also recognized the importance of persuasion theory in examining how technology influences attitudes and behaviours. To address the complexity of the persuasion literature, efforts have been made to develop a common frame of reference for conceptualizing persuasion and differentiating it from related concepts in IS research [17]. Principles of Persuasion are fundamental concepts in social psychology and communication that explain how individuals can influence others' attitudes and behaviours. These principles can be applied to various contexts, including mass persuasion, as explored by [18]. Cialdini (1993) identified six universal principles of influence, which have become widely recognized in the field. These key principles, known as the theory of influence, claimed as encompassing all human persuasion techniques: 'Authority,' 'Reciprocity,' 'Commitment' and 'Consistency,' 'Social Proof,' 'Liking and Similarity,' and 'Scarcity' [19]. In 2003, Gragg examined the psychological triggers that contribute to the success of social engineering, such as: 'Strong Affect,' 'Overloading,' 'Reciprocation,' 'Deceptive Relationships,' 'Diffusion of Responsibility' and 'Moral Duty,' 'Authority,' and 'Integrity' and 'Consistency' [20]. In 2009, Stajano and Wilson analysed various scams that were investigated, documented, and recreated for a BBC TV program. They identified general principles based on recurring victim behaviour patterns that scammers exploit. These principles include 'Social Compliance,' 'Herd,' 'Deception,' 'Dishonesty,' 'Time,' 'Need and Greed,' and 'Distraction' [21]. Together, these studies provide a comprehensive understanding of persuasion techniques and their applications in various domains. The Principles of Persuasion are influential factors in human decision-making, applicable in various contexts including marketing, social engineering, and phishing attacks [22].

A. Unique list of Principles of Persuasion in Social Engineering

Ferreira and Teles (2019) proposed developing a comprehensive list of persuasion principles to understand how phishing emails influence users and bypass security measures. They created a unique list of persuasion principles in social engineering by analysing the relationships between the works of Cialdini (2007), Gragg (2003), and Stajano and Wilson (2011). The final list includes five principles, collectively named the Principles of Persuasion in Social Engineering.

P1: 'Authority' - Society conditions individuals to obey authority without question [11]. People typically follow an expert or an authoritative figure and will go to great lengths for someone they perceive as being in charge [11]. For example, an email that appears to be from the recipient's bank and includes the bank's name in the subject line exploits this principle.

P2: 'Social Proof' - People often follow the actions of the majority, lowering their guard and suspicion to share the same responsibilities and risks [11]. This way, they avoid sole accountability if something goes wrong [11]. For example, an email from a purported system administrator with a company email address asks the recipient to test a link, claiming that their colleagues are also testing it.

P3: 'Liking and Similarity', and 'Deception' - People are more inclined to follow or relate to individuals they know, like, find attractive, or perceive as like themselves [11]. However, appearances can be deceiving, and individuals are often manipulated into believing false identities [11]. For example, an email from someone pretending to be a friend of the recipient, asking them to visit an interesting website, exploits this principle.

P4: 'Distraction' - When people are preoccupied with potential gains, losses, urgent needs, intense emotions, or the scarcity of an item, they often overlook other important factors in their decision-making [11]. For instance, an email claiming the recipient has won a large lottery prize can make them focus on how to claim the money, distracting them from realizing they never bought a lottery ticket in the first place.

P5: 'Commitment', 'Integrity,' and 'Reciprocation' - People often feel compelled to reciprocate a favour or respond to an action due to a sense of commitment to a previous interaction [11]. Additionally, they generally trust that the person they are communicating with is being honest about their needs or feelings [11]. For example, an email from someone who knows the recipient is house hunting and offers a great deal on a property that matches the recipient's criteria. To secure the property ('Commitment'), the recipient must urgently pay a deposit ('Reciprocation').

They also detailed the sub-principles that these main principles encompass or intersect with. The email content analysis framework, including the coding tree and codes are based on those definitions.

III. IDENTIFYING PRINCIPLES OF PERSUASION IN PHISHING EMAIL CONTENT

To investigate the use of Principles of Persuasion in phishing emails, a sample of phishing emails was selected for analysis using qualitative content analysis. The following sections outlines methodology used for the sampling process and the procedures for analysing how Principles of Persuasion are utilized in these emails.

A. Sample and criteria

The phishing emails sample was sourced from the millersmiles online platform (millersmiles.co.uk), a widely recognized and freely accessible anti-phishing service. Known internationally, millersmiles is a prominent repository for information on spoof emails and phishing scams. It maintains an extensive archive of these scams, making it a leading resource on the internet for anti-phishing efforts [23]. Utilizing this reliable archive ensures a higher level of confidence in the authenticity and validity of the included phishing email samples.

Regarding the sampling process, a 10-year timeframe from 2014 to 2023 was chosen to mitigate biases associated with trends specific to individual years. Within this timeframe, 20 phishing emails per year were selected, a total of 200 emails were selected for analysis, with 20 emails sampled from each year. This sample size aligns with common practices [11] [14] in phishing email research, where studies typically analyse between 200 to 250 samples based on literature findings. Additionally, analysis of variability indicated that consistent patterns emerged after examining 180 samples, thus confirming the decision to include 200 samples. The emails included in the study were randomly chosen using a randomized selection method.

B. Analysis of email content

The email contents underwent content analysis using NVivo 14 software. The analysis involved categorizing the phishing email samples by the year of origin. Additionally, each sample was classified based on its target: if aimed at an individual, it was labelled as Individual; if directed at an organization, it was categorized as Organization. Furthermore, the data were classified according to the goal of each phishing email sample, which included categories such as Financial Gain, Service Interruption, and Unauthorized Access. The final coding tree and code definitions were established deductively, meaning they were grounded in existing theory and based on the Principles of Persuasion defined by Ferreira and Teles (2019), rather than emerging inductively from the data. In the coding tree, 'Parent' codes represent broader concepts or principles that encompass a set of 'Child' concepts or principles. For instance, 'Social Proof' includes 'Herd', 'Diffusion of Responsibility' and 'Moral Duty'. Additionally, 'Parent' codes can also represent concepts or principles that intersect with others but are not contained within any broader concept or principle, such as 'Integrity'. 'Child' codes, therefore, refer to the specific concepts or principles that fall under 'Parent' codes. In the coding process, semantic texts, specifically themes, were chosen as the units of record, meaning that content segments, including multiple excerpts from a single sentence line, could be coded into different categories. The results are presented using absolute frequencies, showing the number of references coded according to Principles of Persuasion, sub-principles, and attributes based on the goals of the phishing emails. Additionally, graphical representations of the data illustrate keyword frequencies through word frequency queries or word clouds. The analysis and reporting of results will emphasize absolute frequencies and percentages within categories to visually represent elements found in the sample of phishing emails.

IV. PERSUASION IN PHISHING EMAIL CONTENT

This section provides the results from the content analysis conducted on the sample of phishing email content, using the predefined deductive coding tree.

A. Word Frequency

Fig. 1. Word cloud showing the most frequently occurring words in the phishing email content

As shown in Figure 1, a word frequency analysis was conducted to visualize the 50 most common words or concepts in the whole phishing email content. To avoid redundancy, stemmed words (e.g. update, updated, updating)

were considered in the analysis. Additionally, conceptually irrelevant words (e.g. from, what's) were added to the stop words list. The resulting word cloud highlighted that many frequent terms suggested the use of Principles of Persuasion such as 'General Deception', with words like 'account' (n = 437) and 'emails' (n = 139) standing out. The presence of words like 'update' (n = 129) or 'information' (n = 110), implying that something is being offered to the recipient, pointed to the use of the 'Reciprocation' principle of persuasion. Other terms, such as 'please,' 'security,' and 'dear,' indicated the use of the 'Integrity' principle. Banking-related terms, financial institutions, well-known company names, and email service provider names were frequently employed as authority figures.

B. The Principles of Persuasion in phishing email content

The content analysis was conducted on 200 phishing email samples. By analysing the content of these emails, it was found that the most prominent principle of persuasion, based on the number of references coded, was the principle of 'Distraction,' with a total of 537 references. Those references were distributed across 171 email sample files, with some files containing more than one distraction-suggesting text element. Excerpts coded under this category indicate the use of 'Distraction' based on 'Need & Greed' (n=63), 'Overloading' (n=180), 'Scarcity' (n=103), and 'Strong Affect' (n=191). The use of warning expressions or terms eliciting alertness (e.g., 'alert,' 'important,' 'limited') was the most frequent practice identified in this category. Additionally, some expressions were used to elicit shock and overload recipients with information to create distraction.

The second most prominent principle of persuasion identified in the analysis was 'Deception,' with 520 references across 171 files. This principle encompasses 'General Deception' (n=228), 'Deceptive Relationships' (n=121), and 'Liking and Similarity' (n=171). 'General Deception' involves manipulation without establishing relationships (e.g., "Due to a recent security issue, your account is temporarily deactivated"). Some examples of 'Deceptive Relationships' involve creating false shared interests to foster favourability (e.g., "Dear valued customer, your account details need to be updated"). In the 'Liking and Similarity' category, text units leverage familiarity, likability, or shared interests to persuade (e.g., "Your email service won't be affected and you'll keep all your old contacts, folders, and messages," or "Your NatWest Credit Card Online Services security details were recently changed").

The third most prominent principle of persuasion was 'Integrity,' with 507 references across 170 files. This principle includes 'Reciprocation' (n=211), 'Integrity' (n=106), 'Consistency' (n=102), and 'Commitment' (n=88). The excerpts mainly involve evoking security cues and suggesting offers of information or favours to the email recipient (e.g., "please kindly click here now to restore your old secure password," "verify apple account, this is an automated message"). These tactics aim to make recipients feel secure about replying to emails or clicking provided links, despite the potential security risks, unless there is convincing evidence to the contrary.

The fourth most prominent principle of persuasion was 'Authority,' with 196 references across 116 files. Excerpts coded under this category suggest the use of authority figures, such as known organizations, or authority cues, such as the imperative form to issue orders. References to known organizations as authority figures were particularly notable for financial or finance-related entities (e.g., PayPal, Chase, NatWest, Bank of America, FirstBank, MoneyGram, American Express). Additionally, technology companies (e.g., Apple, Microsoft, Google, Dropbox), email service providers (e.g., Yahoo, AOL, Bigpond), and other companies offering products and services (e.g., Amazon, Wells Fargo, Verizon, Netflix, FedEx, Walmart) were also used to capture the recipient's attention.

Table I illustrates the salience of each principle of persuasion, sorting them in descending order according to the number of references coded and the number of source files where the principles were identified. Considering the deductively defined coding tree, some Principles of Persuasion were identified very infrequently in the content analysis of the 200 emails, namely: 'Social Proof' (P2); 'Herd' (P2.1); 'Moral Duty' (P2.3); and 'Diffusion of Responsibility' (P2.2). Therefore, based on this analysis, conclusions cannot be drawn regarding the employment of these principles in phishing emails.

TABLE I. Absolute Frequencies of References Coded by Principles

Main Principle	Sub-Principle	Files	References
Distraction (P4)		171	538
	Strong Affect (P4.3)	110	191
	Overloading (P4.2)	115	180
	Scarcity (P4.1)	68	103
	Need and Greed (P4.4)	41	63

Main Principle	Sub-Principle	Files	References
Deception (P3)		175	530
	General Deception (P3.1)	115	228
	Liking and Similarity (P3.3)	98	171
	Deceptive Relationships (P3.2)	101	121

Main Principle	Sub-Principle	Files	References
Integrity (P5)		170	508
	Reciprocation (P5.4)	129	211
	Integrity (P5.1)	74	106
	Consistency (P5.2)	67	102
	Commitment (P5.3)	68	88

Main Principle	Sub-Principle	Files	References
Authority (P1)		116	196

Main Principle	Sub-Principle	Files	References
Social Proof (P2)		7	16
	Herd (P2.1)	7	7
	Moral Duty (P2.3)	7	7
	Diffusion of Responsibility (P2.2)	1	1

Similarly, as shown in Figure 2, the Principles of Persuasion with the highest percentage of the sources' content (200 emails) were 'Deception' (27.39%), 'Distraction' (26.76%), 'Integrity' (26.60%), 'Authority' (18.15%), and 'Social Proof' (1.10%).

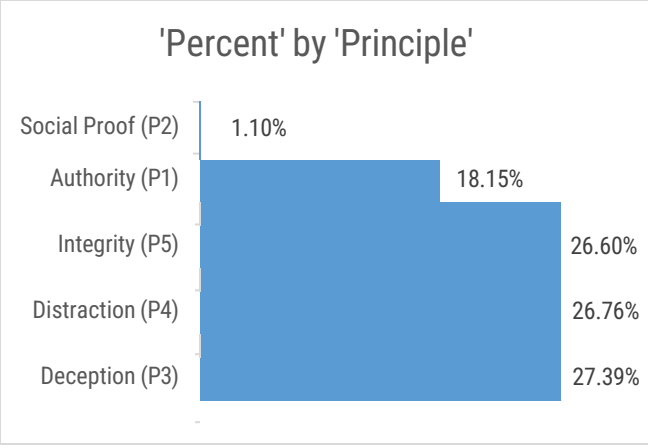

Fig. 2. Percentage of the file source (200 phishing emails) covered in each principle of persuasion category.

V. TARGET AND GOALS OF THE PHISHING EMAILS

According to the Ontological Model of Mouton (2014) in the social engineering attack framework, a social engineering attack target can be an individual or an organization. In this study, phishing email samples were classified according to their target. All of the phishing email samples were targeted at individuals, with very few targeting organizations. Moreover, the Ontological Model of Mouton (2014) identifies three goals of social engineering attacks: 'Financial Gain,' 'Unauthorized Access,' and 'Service Disruption' [24]. As shown in Figure 3, among these goals, 60% of the phishing emails aimed for 'Unauthorized Access', and 39% aimed for 'Financial Gain.' Very few phishing emails targeted 'Service Disruption,' indicating that most phishing emails aim for 'Financial Gain' and 'Unauthorized Access' to sensitive information, which can be misused for monetary gain.

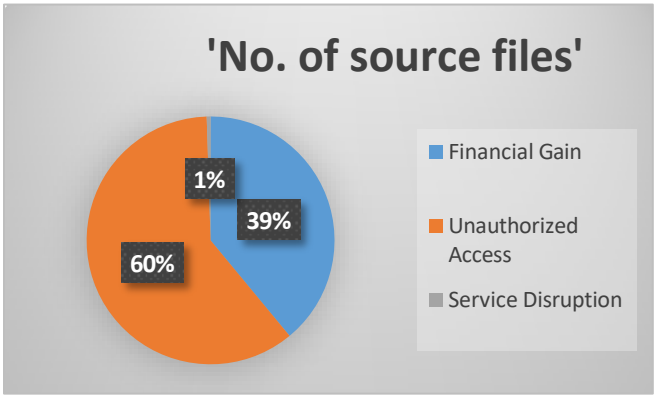

Fig. 3. Goal of the phishing email samples

VI. DISCUSSION

This study builds on previous research by Ferreira and Teles (2019), which synthesized three research works ([19]; [20]; [21] to propose a unique list of Principles of Persuasion in social engineering. While Ferreira and Teles (2019) experimented with email subject lines, this study analysed the entire email content. Additionally, this study uniquely examined the goals and targets of phishing email samples, which is a novel contribution to the field. If this study's result is applied to the ontological model by Mouton et al. (2014), when social engineers use email as a medium for phishing, the primary targets will be individuals. The goals of these social engineering attacks are likely to be 'Unauthorized Access' more often than 'Financial Gain,' followed by 'Service Disruption.' Furthermore, as a compliance principle, 'Distraction' will be the most commonly used technique. Studying human persuasion in dialogues and interactions mediated by technology can aid in developing complementary methods to detect and discard phishing emails, preferably before they reach the user [11]. While luring elements in phishing emails have been previously identified, findings from empirical research in this field have often been conflicting [11]. For instance, Akbar (2014) identified 'Authority' and 'Scarcity' as the most common persuasion principles, whereas Ferreira et al. (2015) found 'Liking and Similarity' to be the

most frequent. In this study, 'Distraction' was the most commonly used principle of persuasion, followed by 'Deception,' 'Integrity,' and 'Authority.' Consequently, this paper provides additional insights into the luring elements of phishing emails. Ferreira and Teles (2019) conducted a study analysing email subject lines, which was their novel approach. In the same paper, they suggested that analysing the entire email text could identify additional Principles of Persuasion, a gap that this paper aims to fill.

VII. CONCLUSION

This study analysed the entire email content to identify principles of human persuasion within phishing emails. It demonstrates why phishing email content can be useful for automated detection and prevention. The author suggests that future solutions should focus on leveraging socio-technical principles such as 'Distraction,' 'Deception,' 'Integrity,' and 'Authority.' Future work will involve applying this methodology to other social engineering attack techniques beyond phishing emails, in conjunction with the ontological model of social engineering, to provide further insights to the research community.

REFERENCES

[1] K. Khadka, A. B. Ullah, W. Ma, E. M. Marroquin, and Y. Alem, "A Survey on the Principles of Persuasion as a Social Engineering Strategy in Phishing," in *2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 1-3 Nov. 2023 2023, pp. 1631-1638, doi:10.1109/TrustCom60117.2023.00222. [Online]. Available: https://ieeexplore.ieee.org/document/10538702/

[2] S. Gupta, A. Singhal, and A. Kapoor, "A literature survey on social engineering attacks: Phishing attack," in *2016 International Conference on Computing, Communication and Automation (ICCCA)*, 29-30 April 2016 2016, pp. 537-540, doi: 10.1109/CCAA.2016.7813778. [Online]. Available: https://ieeexplore.ieee.org/document/7813778/

[3] A. Sumner and X. Yuan, "Mitigating Phishing Attacks: An Overview," *Proceedings of the 2019 ACM Southeast Conference*, 2019.

[4] A. Kamruzzaman, K. Thakur, S. Ismat, M. L. Ali, K. Huang, and H. N. Thakur, "Social Engineering Incidents and Preventions," in *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*, 8-11 March 2023 2023, pp. 0494-0498, doi: 10.1109/CCWC57344.2023.10099202.

[5] R. Taib, K. Yu, S. Berkovsky, M. Wiggins, and P. Bayl-Smith, "Social Engineering and Organisational Dependencies in Phishing Attacks," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, D. Lamas, F. Loizides, L. Nacke, H. Petrie, M. Winckler, and P. Zaphiris, Eds., 2019, vol. 11746 LNCS: Springer Verlag, pp. 564-584, doi: 10.1007/978-3-030-29381-9_35. [Online]. Available: https://www.scopus.com/record/display.uri?eid=2-s2.0-85072862692&doi=10.1007%2f978-3-030-29381-9_35&origin=inward&txGid=a82e14432f144cc928529e06ae38a7f9

[6] M. Alsharif, S. Mishra, and M. AlShehri, "Impact of Human Vulnerabilities on Cybersecurity," *Computer Systems Science and Engineering*, vol. 40, no. 3, pp. 1153-1166, 2022. [Online]. Available: https://www.techscience.com/csse/v40n3/44582.

[7] S. Goel, K. Williams, and E. Dincelli, "Got phished? Internet security and human vulnerability," *Journal of the Association for Information Systems*, vol. 18, no. 1, p. 2, 2017.

[8] N. Y. Conteh and M. D. Royer, "The rise in cybercrime and the dynamics of exploiting the human vulnerability factor," *International Journal of Computer (IJC)*, vol. 20, no. 1, pp. 1-12, 2016.

[9] A. Pollini *et al*., "Leveraging human factors in cybersecurity: an integrated methodological approach," *Cognition, Technology & Work*, vol. 24, no. 2, pp. 371-390, 2022/05/01 2022, doi: 10.1007/s10111-021-00683-y.

[10] ACCC, "Scam Statistics," Australian Government, 07 June 2024 2024.

[11] A. Ferreira and S. Teles, "Persuasion: How phishing emails can influence users and bypass security measures," (in English), *International Journal of Human Computer Studies*, Article vol. 125, pp. 19-31, 2019, doi: 10.1016/j.ijhcs.2018.12.004.

[12] F. Hassandoust, H. Singh, and J. Williams, "The Role of Contextualization in Users' Vulnerability to Phishing Attempts," 2020.

[13] D. Kim and J. Hyun Kim, "Understanding persuasive elements in phishing e-mails," *Online Information Review*, vol. 37, no. 6, pp. 835-850, 2013, doi: 10.1108/OIR-03-2012-0037.

[14] N. Akbar, "Analysing persuasion principles in phishing emails," University of Twente, 2014.

[15] A. J. Almagsosi and K. H. Alghezzy, "PERSUASION IN MEDIA," 2020.

[16] J. K. Clark, "Antecedents of Message Processing in Persuasion: Traditional and Emergent Perspectives," *Social and Personality Psychology Compass*, vol. 8, pp. 595-607, 2014.

[17] P. Slattery, R. T. Vidgen, and P. Finnegan, "Persuasion: An Analysis and Common Frame of Reference for IS Research," *Commun. Assoc. Inf. Syst.*, vol. 46, p. 3, 2020.

[18] D. Cartwright, "Some Principles of Mass Persuasion," *Human Relations*, vol. 2, pp. 253-267, 1949.

[19] R. B. Cialdini, Influence: *The psychology of persuasion*. Collins New York, 2007.

[20] D. Gragg, "A multi-level defense against social engineering," *SANS Reading Room*, vol. 13, pp. 1-21, 2003.

[21] F. Stajano and P. Wilson, "Understanding scam victims: seven principles for systems security," *Communications of the ACM*, vol. 54, no. 3, pp. 70-75, 2011.

[22] A. Ferreira, L. Coventry, and G. Lenzini, "Principles of Persuasion in Social Engineering and Their Use in Phishing," Springer International Publishing, 2015, pp. 36-47.

[23] Millersmiles. *Phishing Scams and Phishing Reports at MillerSmiles.co.uk*. [Online]. Available: millersmiles.co.uk

[24] F. Mouton, M. M. Malan, L. Leenen, and H. S. Venter, "Social engineering attack framework," in 2014 *Information Security for South Africa*, 2014: IEEE, pp. 1-9.