



A classification of manipulation technique used in social engineering attacks and underlying cognitive biases, needs, norms, and emotions

Antony Dalmiere, Vincent Nicomette, Guillaume Auriol, Pascal Marchand

► To cite this version:

Antony Dalmiere, Vincent Nicomette, Guillaume Auriol, Pascal Marchand. A classification of manipulation technique used in social engineering attacks and underlying cognitive biases, needs, norms, and emotions. 2025. <hal-05027416>

HAL Id: hal-05027416

<https://hal.science/hal-05027416v1>

Preprint submitted on 9 Apr 2025

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



HAL Authorization

A classification of manipulation technique used in social engineering attacks and underlying cognitive biases, needs, norms, and emotions

ANTONY DALMIERE, CNRS, France

VINCENT NICOMETTE, CNRS, France

GUILLAUME AURIOL, CNRS, France

PASCAL MARCHAND, LERASS, France

This survey addresses the critical challenge of social engineering attacks in cybersecurity, offering a detailed classification of manipulation techniques and an exploration of the cognitive processes they exploit. We identify 45 distinct manipulation techniques by integrating insights from social and cognitive psychology literature, focusing on cognitive biases, social norms, individual needs, and emotions. Our analysis reveals that techniques frequently employ cognitive biases such as the halo effect and individual needs like the need for affiliation to deceive users. We provide practical examples of how these techniques manifest in phishing and spear-phishing campaigns, underscoring their relevance to current cybersecurity threats. Our findings underscore the necessity for cybersecurity defences that incorporate psychological insights, aiming to enhance user awareness and resilience against these sophisticated attacks. This survey lays the groundwork for future research and practical applications in combating social engineering, ultimately contributing to the fortification of information systems against human-centric vulnerabilities.

Key Words: social engineering, phishing, user, human security, cognitive bias, social norms, need for, psychology

1 INTRODUCTION

Cybersecurity poses a significant concern for industry, governments, and citizens in the digital era. Computer assaults have increased in number and variety, targeting software, equipment, network protocols, and the human mind. Each part of an IT system comes under fire, with all areas of application being impacted, especially critical sectors that face escalating threats, such as transportation, energy, healthcare, and communication. Hackers' objectives do not focus solely on financial gain, and resultant negative impacts extend beyond financial losses to include interference in democratic processes [27] and even homicide [45].

Every year, an increasing proportion of cyber incidents target humans, with more than 800,000 occurring in 2016 [65], up from 200,000 in 2010. A most recent study [40] also confirms that 83% of the cyberattacks targeting UK business organizations in 2023 were phishing attacks. These cyberattacks have a significant impact on various organizations [167], including the 2016 US presidential elections. Hillary Clinton's campaign manager was targeted by a phishing attack, allowing access to her campaign emails [96]. France was also affected in 2017 when internal emails from the president's political party were exposed on the eve of the elections following a phishing attack on an official [128]. To cite another example, Bangladesh's central bank suffered a \$81 million fraud due to an intrusion into its banking network following a phishing attack to obtain SWIFT network login credentials [185].

Given these significant threats, it is crucial to devise reliable and efficient user-oriented solutions that safeguard information systems. Extensive research is currently underway to develop appropriate cybersecurity defense mechanisms. However, these defense mechanisms do not cover the human weaknesses that are successfully exploited by social engineers through *social engineering attacks*.

Professionals in the field of cybersecurity must keep themselves up-to-date to counter these attacks, which are primarily aimed at cognitive systems (a.k.a. user mind), all the more as social engineering tools continually evolve [199]. Everyone agrees to know that it is often simpler to manipulate a human than to execute a purely technical attack, which must bypass multiple layers of protection [122, 143, 162]. Various models concentrate on various aspects of cyberattacks [129], like Advanced Persistent Threats [15, 18, 56, 77, 112, 134], but in the business sector, phishing represented 33.6% of attacks directed towards UK organizations [5] in 2018 and 2019, and up to 83% in 2023 according to a recent study [40]. This is particularly worrying given that the success rate of these attacks ranges from 23% to 59% depending on the level of targeting, manipulation techniques and communication channels [8, 9, 61, 88, 137]. Despite the fact that people are responsible for 82% of data breaches [179], the countermeasures being implemented [5] are predominantly technical only, such as updating policies and installing antivirus software, and establishing firewall rules.

These technical countermeasures are not effective against social engineering attacks. Contemporary defensive strategies must prioritize the human element over the technological. Various domains of research are well-suited to address this paradigm, including Human Factor Engineering [152], which concentrates on the dynamics between users and their devices, and User Education, which has demonstrated considerable potential [26, 183, 198]. Nevertheless, the literature concerning the offensive techniques employed by adversaries to exploit users is not as extensive as the aforementioned research field. This is unfortunate, as the distinction between a rudimentary defense and a comprehensive defense-in-depth is predicated upon an understanding of the offensive tactics.

Updated cyberattacks are no longer basic and simple as they were ten years ago, when social engineers promised to win millions of dollars just by replying to an email. Nowadays, social engineers use enhanced psychological vulnerabilities to increase the effectiveness of their strategies [68, 122, 167]. These manipulative techniques specifically exploit the

target's cognitive processes [93]. This is all the more important than social engineering attacks become more and more difficult to detect and counter, even for people aware of cybersecurity issues. The time when the phishing emails were really obvious to detect is over. Even if some of them still exist, a lot of really carefully designed phishing attacks exist now, which are fearsomely efficient [20].

The objective of this survey is to inventory, detail and characterize manipulation techniques employed by social engineers, based on a comprehensive review of the literature in social and cognitive psychology. Some research papers from the cybersecurity literature propose taxonomies of manipulations techniques (we present some of them in the beginning of this paper), but to our knowledge, this paper is the first to carry out such a thorough study, analysing the literature in social and cognitive psychology from the perspective of cybersecurity and social engineering in particular. This perspective enables to propose a richer classification, because the other taxonomies suffer from insufficient consideration and understanding of the underlying human cognitive processes, which is a crucial factor in the process of a social engineering attack. We argue that such a study is essential from different perspectives : 1) for the researchers in computer science so that they may better understand the strategies of the social engineers to reach a specific goal and so that they may propose better appropriate defense solutions ; 2) for the different actors in the cybersecurity domain, such as security product suppliers, political and economic decision-makers who are responsible for setting the policies, regulations, and standards for cybersecurity in various sectors and domains; 3) for the end-users themselves, so that they are more aware of the different manipulation techniques used by the social engineers and so that they may adopt more secure behaviours when they are facing such attacks. Let us emphasize that such a survey is not quite easy to carry out, as it requires the cooperation of authors that both understand two different worlds : the world of social and cognitive psychology and the world of computing science. We then made the effort to produce this survey by bringing scientists of these two worlds around the table.

In this survey, it was also important for the authors to avoid the catalog effect of presenting all the manipulation techniques used by the social engineers one after the other. For that purpose, we decided to rely on a specific model (from the literature in psychology also) of the information processing that is performed by a target when he is facing a social engineering attack. The information processing is performed in different stages according to this model, and we present the different manipulation techniques employed by the social engineers according to the stage of the information processing in which they are used.

The presentation of these manipulation techniques is crucial, but another important issue is to understand the underlying cognitive processes that are employed in the manipulation techniques. In this survey, we also propose a classification of these different cognitive processes (cognitive biases, social norms, individual needs and emotions) and describe the relationships that exist between the manipulation techniques and these cognitive processes. The exploration of the underlying cognitive processes is fundamental because they characterize the human vulnerabilities that are exploited by the attackers. This knowledge is notably essential to establish countermeasures to the manipulation techniques.

To sum up, the two main contributions of this survey are:

- (1) The presentation of the manipulation techniques that are used by social engineers, based on a detailed analysis review of the literature in social and cognitive psychology. The different manipulation techniques are presented according to the stage of the information processing in which they are used by the social engineer (these different stages are based in a specific model of information processing proposed in the literature in social and cognitive psychology)

- (2) The presentation and classification of the different cognitive processes that are employed by the manipulation techniques and the relationships between the processes and the manipulation techniques.

Let us note that the purpose of this survey is not to provide quantitative metrics on the number of attacks per manipulation technique that have been published so far. This survey aims at providing a classification as exhaustive as possible of the manipulation according to the review of the literature, regardless of whether they have been used or not so far by the social engineers.

This survey is structured as follows. In Section 2, we present some taxonomies of manipulation techniques that are used in the cybersecurity literature and explain why these taxonomies, even if relevant, are not sufficient. In Section 3, we provide detailed descriptions of the 40 manipulation techniques identified in the literature in social and cognitive psychology, acknowledging that there may be techniques not yet employed, but likely to be used in the future by social engineers. Section 4 summarizes the cognitive processes used in manipulation techniques and classifies them into categories. Lastly, Section 5 discusses the limitations, challenges and future scope of our work.

2 REPRESENTATIONS OF MANIPULATION TECHNIQUES IN CYBERSECURITY LITERATURE

In recent years, various conceptual models and taxonomies have been developed to describe phishing and social engineering attacks [47, 60, 127, 182]. Although some of these representations deal with social engineering as a whole and recognize the importance of psychological aspects, they often suffer from a lack of accuracy on cognitive processes because they are focus on computer science and make little use of the literature in social and cognitive psychology. Consequently, an exhaustive understanding of the psychological levers exploited is lacking, and the proposed representations remain superficial from a social science point of view. However, some of these representations may be widely popular, operational, or empirically valid, so it is important to describe them and identify how they can be improved [30, 47, 60, 127, 182].

The Cialdini taxonomy [30] summarizes the primary principles and techniques of social influence derived from decades of psychological research. It outlines six crucial factors that can enhance compliance with a request: *Reciprocation*, *Commitment and Consistency*, *Social proof*, *Liking*, *Authority* and *Scarcity*. The article provides a thorough overview of the mechanics, effectiveness, and ethical implications of persuasion tactics employed by marketers, advertisers, salespeople, and fundraisers. It also provides various examples and studies to illustrate the application and impact of these factors in different domains and contexts. The article, drawing from numerous sources and disciplines, presents a clear and comprehensive account of the science of persuasion. The text offers practical and pertinent advice for both persuaders and persuades, enhancing their understanding and improving their decision-making and influencing skills. Nonetheless, the article only covers few techniques: *Reciprocity*, *Fake Consistency*, *Flattery*, *Foot in the door*, *Scarcity*, *Social Pressure*, *Time Pressure*, *Humour*, *Group Thinking*, *Similarity*, *Include half-confidential detail*, *Attractiveness*, *Authority*, *Fake divergence*. This can be explained because Cialdini's goal was to highlight and exemplify only technique usable in marketing and sales context. For the same reason, consideration of the possible interactions or conflicts between the six factors, or even the role of other factors that may influence compliance, such as emotions, personality and situational factors are overlooked.

The taxonomy of Gragg [60] proposes a comprehensive framework for protecting people at organization scale from social engineering attacks. The paper defines social engineering as the process of tricking people into giving up access or confidential information, and identifies the psychological triggers that make it successful, such as *Strong Affect*, *Overloading*, *Reciprocation*, *Deceptive Relationships*, *Diffusion of Responsibility and Moral Duty*, *Authority* and *Integrity*

and Consistency. The paper then proposes a layered defense that addresses these triggers and consists of six layers: security policy, security awareness training, resistance training, ongoing reminders, social engineering landmines and incident response. The paper also introduces the concept of social engineering landmines (SELMs), which are procedures or policies that act as an intrusion detection system for social engineering and bait the social engineer. It also provides a practical and detailed framework for defending against social engineering, covering both preventative and reactive measures. However, because that paper is defense oriented, the psychological trigger used during an attack are not explained through any psychological framework and not linked with any empirical examples.

Taxonomy of Ferreira et al. [47] compares and merges different conceptual models and taxonomies of persuasion that can be used in social engineering and phishing attacks. The article reviews the work of Cialdini [30], Gragg [60], Stajano et al. [168] and identifies the common and distinct principles of influence, psychological triggers, and principles of deception that they propose. The article subsequently condenses a roster of five principles of persuasion in social engineering, specifically: *Authority, Social proof, Liking, Similarity and Deception, Commitment Reciprocation & Consistency*, and *Distraction*. The article examines a selection of phishing emails and identifies the most used principle as *Liking, Similarity & Deception*. It offers an empirical view of the principles it presents and explains how they relate and overlap, which is the only one to do this. However, it omits the interactions of the influence of other factors, for instance, emotions, personality, or situational elements, that might impact phishing incidents. Moreover, given that taxonomy is build on top of other taxonomies [30, 60, 168] which already have low granularity, this taxonomy also lacks of granularity and the *Distraction* principle corresponds to more than half of the techniques mapped in this survey.

The taxonomy of Wang et al. [182] explores the psychological and behavioural aspects of social engineering attacks. The article proposes a conceptual model that describes how social engineering attacks work based on three core entities: effect mechanism, human vulnerability, and attack method. The article examines the diverse effect mechanisms categories that social engineering can employ including persuasion, social influence, cognition and attitude and behaviour, trust and deception, language and thought and decision, emotion and decision-making. Each of these categories contains between four and nine effect mechanisms. The paper additionally showcases 16 examples of social engineering attacks, demonstrating the practical application and combination of these principles. Nonetheless, the article lacks of understanding and meticulous evaluation of the validity or reliability of the conceptual model because it places taxonomies, models and empirical studies at the same level of *effect mechanism* or *human vulnerabilities*. For example, it identifies *peripheral route to persuasion* and *emotion and feelings influence decision-making* as effect mechanisms, even though the first one is a part of a model [147] and the second one is the result of an empirical study [85]. At times, some concepts identified as different have in fact an inclusion relation which sometime leads to blurring the conceptual boundaries and definitions of various psychological concepts, and may merge or split them arbitrarily.

Taxonomy of Montanez & Xu [127] presents a methodical framework for modeling and characterizing cyber social engineering (CSE) attacks that exploit human factors to compromise security. It links literature in social and cognitive psychology to the well-known cyberattack frameworks Lockheed-Martin Cyber Kill Chain [112] and MITRE ATT&CK framework [36]. The article is the sole one that links the CSE Kill Chain with existing cyberattack frameworks, easing the integration and alignment of social engineering and technological attacks. The CSE Kill Chain framework is introduced, which outlines the four stages of social engineering attacks: pre-stage, resource development, execution, and exploitation. Each phase is made up of several tactics composed of techniques derived from the psychological constructs that influence human information processing: trust, framing, persuasion, deception, risk acceptance, and attention. The article exemplifies the framework's value by employing it to examine a real-world attack. The author overlooks the victim's and environmental factors because it is not the goal of their framework, even if they already depicted

these aspects in one of their previous article [126]. Also, the *psychological construct* which is the base of the technique depicted in the paper does not rely on an extensive review of the literature in social and cognitive psychology, which leads technique *CSE-T1108* aka also named *Persuasion* to be the most represented technique due to its vague description. Another consequence of the choice of very restricted psychological constructs is the impossibility to identify techniques that do not exploit the few constructs chosen.

To summarize, the existing taxonomies have achieved a reasonable level of coverage when it comes to techniques found in the realm of social influence and social engineering, as exemplified by Kim [91]. However, it is important to note that broader coverage does not necessarily equate to adequate granularity. Notably, taxonomies such as those proposed by Gragg [60], Ferreira et al. [47], and Wang et al. [182] exhibit a tendency to identify various techniques as similar, despite their reliance on distinct cognitive processes. In contrast, Cialdini's taxonomy [30] offers substantial supporting evidence but falls short in terms of comprehensively covering social engineering attacks. On the other hand, the taxonomy developed by Montanez & Xu [127] encompasses a smaller set of techniques compared to the aforementioned taxonomies. However, it possesses a distinct advantage in its integration with the existing MITRE TTP taxonomy, which serves as a valuable contribution to the field. Overall, we consider that these taxonomies can be enriched thanks to the analysis of the literature in social and cognitive psychology, to provide a better fine-grained definition of manipulation techniques, that are employed or not so far by the attackers. In that sense, this research work is useful to anticipate future manipulation techniques that will probably be employed in the near future and that could enrich the MITRE TTP taxonomy.

3 CLASSIFICATION OF PSYCHOLOGICAL MANIPULATION TECHNIQUES

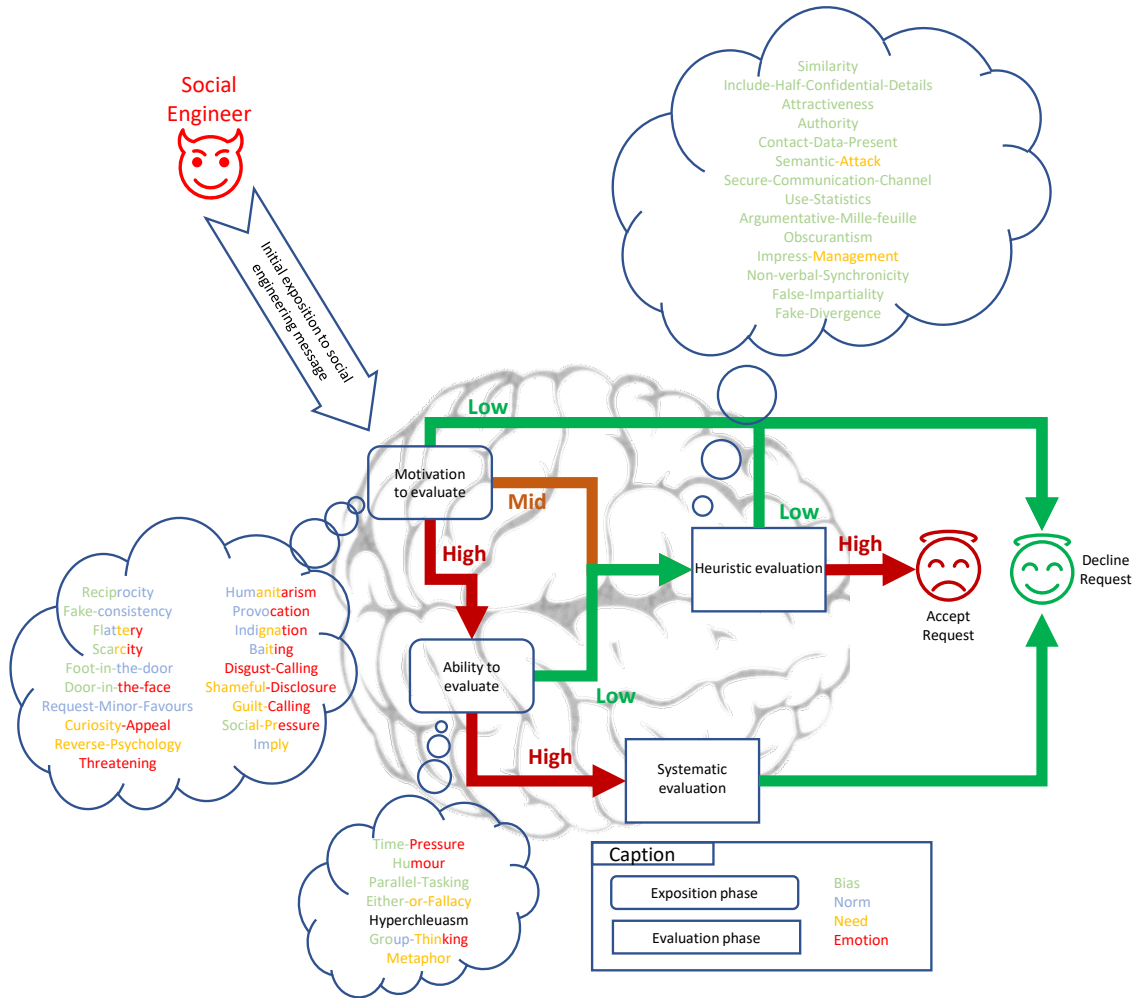
Crafting an exhaustive list of manipulation techniques employed by social engineers is a complex challenge that requires interdisciplinary collaboration. Our research work was focused on a systematic review of the literature in social and cognitive psychology, which revealed that many more manipulation techniques than the ones generally considered by computer scientists, actually exist. We finally identified 40 techniques through the analysis of this literature. But the review of the literature in social and cognitive psychology also highlights that these manipulation techniques are purposely used according to several parameters, and notably the different stages of the information processing of the victim.

More precisely, in this survey, we have adopted dual processing models [28, 147] that describe these stages of information processing. These models, which are comparable and have been modified for social engineering attacks [101, 107, 118, 135, 164], form the basis of our approach and are useful to organize the presentation of the different manipulation techniques. They depict the evaluation of the message, i.e., the stages that the target of a message goes through when receiving a message¹, from a social engineer. They encompass the stages of *Motivation to Evaluate*, *Ability To Evaluate*, *Heuristic Evaluation*, *Systematic Evaluation* (as depicted in Figure 1). At each stage correspond some specific manipulation techniques employed by the social engineer, precisely because they are efficient at this stage.

Let us briefly describe these different stages of the information processing. On first exposure to a message, the target goes through an initial stage of motivation to evaluate the message. This stage determines the cognitive effort that is expended to analyse the message. For instance, a person who is about to receive a parcel is more motivated to process messages about the parcel than an irrelevant advertisement. The motivation stage (*Motivation to Evaluate* in Figure 1) determines whether a target makes significant efforts to evaluate different characteristics of the message conveyed

¹Let us note that the word *message* must be taken in the broad sense: it may be an email message (the larger part of the social engineering attacks), it may also be a message in a social network, an SMS, or even a part of a conversation in a phone call.

Fig. 1. Stages of evaluation of a social engineering message



by the social engineer [67, 194]. According to Metzger [118], individuals process and scrutinize messages to varying depths based on their levels of motivation. When the motivation is not high enough, the message is simply ignored and the request is not met (*No Evaluation* in Figure 1). Alternatively, when motivation is moderate, it is the preferable case for the social engineer as the target enters a state of superficial processing of the message, known as heuristic processing (*Heuristic Evaluation* presented in Figure 1) [28, 118, 146, 147]. This stage is described by Kahneman [86] as a low-energy approach to processing based on simple cues. These cues can be easily falsified by the attacker. If motivation is high, either because of a strong interest in the subject of the message or due to the techniques employed by the attacker, the target's ability (*Ability to evaluate* in Figure 1) to process the message deeply determines the follow-up [118, 146, 147]. If the target lacks the ability, or if the social engineer reduces the target's ability using manipulation

techniques, the target resorts to heuristic processing [118, 142, 147, 180]. If the recipient has the necessary capacity to process the message and their abilities are not limited [118, 139, 146], the target engages in a deeper processing of the message (*Systematic Evaluation* in Figure 1), which requires a great deal of cognitive effort but is much more reliable [86, 118]. This systematic processing determines whether the requests are fraudulent or not, and allows the victim to decline the fraudulent request accordingly. As a consequence, this systematic processing should be avoided by a social engineer. The objective of the social engineer is to disrupt these different stages of message processing by using manipulation techniques to encourage the target to engage in heuristic processing and to influence the outcome of this processing. To achieve this objective, the social engineer uses techniques that influence the target's motivation, ability to evaluate the message, and heuristic processing.

These techniques are presented in Figure 1 in the form of word clouds and are detailed in the following, in Subsections 3.1, 3.2 and 3.3. Furthermore, in Figure 1, each manipulation technique is represented in different colors according to the different underlying cognitive processes associated with this technique. These cognitive processes are described below in Section 4. Let us note that some techniques described below as "double impact techniques" affect several treatment stages at the same time. For each manipulation technique, we provide a simple example of a message (either email content, mail subject, phone call) that could be used by a social engineer. These examples are provided in three Tables 1, 2 and 3. For a few examples, a commentary is added, between brackets.

3.1 Motivation to Evaluate

Techniques that interfere with the motivation to evaluate aim to alter the amount of effort the target puts into processing the message. We have identified these techniques as those that either enhance or reduce the target's motivation. The goal of the social engineer is to achieve a "high" or "mid" level of motivation that results in heuristic processing (as explained in Figure 1). Techniques that increase motivation to evaluate the message give the target a good reason to be interested in the messages. Conversely, techniques that decrease motivation aim to distract attention from the target.

3.1.1 Reciprocity. The *Reciprocity* technique compels the target to sustain interaction through engagement [44, 90]. Initial engagement generates discomfort until rebalanced, encouraging target persistence [90]. The *Reciprocity* technique, which encourages actions by invoking a sense of indebtedness, is effective in marketing [30, 54]. Sales increases follow gift offers [30]. The society (see Section 4.2), as noted by Gouldner [59] encourages people to reciprocate for received favours. Within social engineering, attackers can initiate interaction with a gift, predisposing and amplifying the probability of target re-engagement.

3.1.2 Fake Consistency. The technique of *Fake Consistency* prompts the target to behave consistently with prior, ongoing, or anticipated actions, even if the social engineer fabricates them. This technique capitalizes on cognitive discomfort, known as cognitive dissonance, which arises when actions are incongruous [48]. Consequently, the victim is inclined to maintain an interaction initiated by the social engineer [90]. This technique exploits social norms of consistency [64, 173], aided by verbal or written endorsements [30, 90]. This technique relies on false cues of coherence permitted by the modality of email, in consequence we have found limited research focused on this aspect.

3.1.3 Flattery. The *Flattery* technique is a social engineering method that aims to influence the victim by offering compliments or friendly remarks. It refers to cognitive processes such as feeling indebted to those who have assisted or complimented us [59], the spread of prosocial behaviours following exposure to kindness [62, 84], and the social boost

obtained by social engineers through praise [58, 181]. This technique is widely used in phishing [47, 91], marketing [29, 30], and interpersonal conflicts [22].

3.1.4 Foot-in-the-door. The *Foot-in-the-door* technique aims to achieve compliance with a costly request by initially making a smaller, less demanding request [90]. It relies on commitment, causing the target to feel compelled to accept the second request to maintain consistency with the first [53, 90]. Freedman & Fraser [53] found that this technique increases acceptance rates of demanding requests from 22.2% to 52.8%. It is also used in negotiation to obtain concessions [151]. Baron [12] suggests that the initial request should not be overly demanding to avoid rejection, however a social engineer can ask the target how they feel as the initial request [76].

3.1.5 Door-in-the-Face. The *Door-in-the-face* technique aims to obtain compliance with an expensive request by starting with an unacceptable, excessive request. This technique uses social norms of reciprocity [59, 90] to encourage the victim to make a concession to the social engineer. Cialdini [31] found that this technique increases acceptance rates of demanding requests from 16.7% to 50%.

3.1.6 Scarcity. The *scarcity* technique strategically leverages a fundamental psychological phenomenon: people's innate tendency to attach greater value to items that are not only rare but also elusive in nature, resulting in an artificial amplification of their perceived value [30]. This technique is very common in online sales of limited edition items that are not actually limited. Buyers are looking for items that stand out for their rarity, creating a sense of individuality and exclusivity among ordinary products [100, 108].

3.1.7 Request for Minor Favours. The technique of requesting small favours aims to obtain information or favours by asking for a simple favour that the target is more likely to agree to. This technique exploits the victim's heuristic processing of social engineering requests, especially if the request is perceived as having a low cost [28, 86, 89, 147]. Consequently, the target is likely to respond positively to a request that appears harmless or non-threatening [107], bypassing the need to apply their cybersecurity expertise because it is demanding cognitive efforts. This approach enables the social engineer to decrease motivation to evaluate to avoid systematic evaluation.

3.1.8 Curiosity Appeal. The *Curiosity Appeal* technique is used by social engineers to increase the victim's motivation to evaluate. Curiosity is a factor that influences engagement by driving individuals to actively seek out information on a specific subject, which improves attitude towards this subject [145, 200]. Discomfort prevails until the target satisfies their curiosity by accessing the information [104, 197]. This strategy is effective in phishing attacks, exploiting targets' curiosity, leading them to click malicious links or attachments [97, 131, 154, 182]. Under experimental conditions, this method has a success rate between 60% and 75% in USB drive distribution [8, 169].

3.1.9 Reverse Psychology. The *Reverse Psychology* technique aims to enhance psychological reactance, an individual's resistance to persuasive arguments due to a perceived restriction on their freedom [110]. This approach provokes the target to respond in an opposite way to the attacker's initial proposition [21, 170]. Reactance causes frustration in the target until they regain their autonomy by taking actions that oppose the original proposal, which may include adopting risky or harmful behaviours. Ultimately, the target, motivated by their fundamental desire to protect their freedom, discovers themselves coerced to behave in compliance with the social engineer's actual goal.

3.1.10 Threatening. Double impact technique (see 2.2.7) The *threatening* technique engages the target's emotions by instilling fear [80, 138]. Buss [22] detailed its efficiency in interpersonal relationships, and it is also used in phishing

[73, 91, 122]. Kim & Hyun Kim [91] semantic analysis of 285 emails found that 64.91% of cases use emotion-based appeals. This technique is effective due to the target's innate tendency to restore their compromised sense of security [113]. The social engineer pressures the target into making illogical choices or complying with requests due to fear of negative consequences.

3.1.11 Humanitarianism. The technique of *Humanitarianism* manipulates the target by exploiting emotions of guilt to secure a favourable response or favour. This technique is common in interpersonal relationships, including partnerships, where a partner may depict themselves as a victim to elicit sympathy and compassion [22]. It is especially potent within specific cultural contexts where not offering aid to somebody who has induced guilt is deemed counter-normative [17]. This practice can be seen in deceptive charitable appeals [34].

3.1.12 Provocation. Double impact technique (see 2.2.8) The *Provocation* technique induces anger in the target to increase their motivation to engage with the source of this emotion [55, 99, 138]. This technique, which increases the willingness to take increased risks and engage in impulsive behaviour, is applicable to a variety of contexts and may take the form of a targeted insult directed at the target or their in-group.

3.1.13 Indignation. The *Indignation* technique evokes moderate anger in the target, increasing their motivation to act against perceived injustice [125]. This approach manipulates the target by presenting partial or false facts that contradict their core values or interests. It can be used in various situations, such as making direct statements against the target's beliefs, which lead to increased mobilization and the adoption of activist behaviours. Although this method shares emotional roots with provocation, the level of activation it causes is lower. Therefore, in the absence of studies indicating otherwise, it can be concluded that indignation does not impact the ability to evaluate.

3.1.14 Baiting. Double impact technique (see 2.2.9) *Baiting* is a manipulation technique that uses positive emotional stimuli to attract the target's attention [113]. It can be classified into four subtypes: *Greed Baiting*, *Erotic Baiting*, *Friendship Baiting*, and *Group Baiting*. *Greed Baiting* offers the target an extremely tempting offer, such as a large sum of money [33]. *Erotic Baiting* entices the target with promises of satisfying their sexual desires or romance [186]. *Friendship Baiting* offers the target genuine friendships [113]. *Group Baiting* attracts the target with restricted group membership [113]. These techniques are common in phishing emails [73, 91] and are particularly effective with people who have a strong desire or need for the specific type of pleasure offered as their desire influence their decisions [113, 115].

3.1.15 Disgust Calling. Double impact technique (see 2.2.10) The *Disgust Calling* technique creates a repulsive stimulus, drawing on the emotional response of disgust [80]. This technique is effective because it induces discomfort and aversion in the target, diverting their cognitive resources away from parts of the message [38, 138] like dangers cues. Social engineers use this technique by incorporating disgusting images or content into their communications, leading recipients to partially ignore the message.

3.1.16 Shameful Disclosure. The *Shameful Disclosure* technique uses the powerful emotional force of shame to influence human behaviour [80, 160]. This technique is potent because it induces feelings of self-deprecation in the target, driving them towards actions that conform to societal norms [14]. Its practical implementation involves manipulating the target's vulnerability by threatening to reveal past actions or behaviours that violate societal norms. This technique is used in real-life scenarios such as sextortion [189], where perpetrators use intimate photos or videos to coerce victims into compliance.

3.1.17 Guilt Calling. The technique of *Guilt Calling* manipulates the target by exploiting an internalized sense of remorse and responsibility arising from perceived transgressions [80]. Its effectiveness stems from inducing individuals to act in ways that alleviate their guilt feelings [14, 22]. Social engineers can use this technique by blaming the target for past actions that violate ethical norms, thereby inducing guilt and driving the target to compensatory actions or concessions.

3.1.18 Social Pressure. Double impact technique (see 2.3.8) The technique of *Social Pressure* influences the target by showcasing that others are engaging in that behaviour, even if the group is fictitious [83]. This technique is based on the premise that individuals have a fundamental need to belong to a group or community. When this need is not fulfilled, a state of tension and discomfort can occur [113, 115]. As a result, the target is likely to adhere to the behaviours and attitudes of their social group to secure acceptance and avoid exclusion [6, 111, 172].

3.1.19 Imply. The technique of *Imply* strategically influences the target through subtle suggestions, prompting the target to perceive ideas and objects as self-generated. This tactic is based on individuals' natural inclination to embrace self-generated ideas. Implicit suggestions achieve better outcomes in inducing particular behaviours compared to direct appeals [106, 196]. The increased motivation induced by this approach brings about a more positive attitude towards the subject subtly implied by the social engineer because the target is implicated [105, 200].

3.2 Ability to Evaluate

The ability to evaluate determines the aptitude with which the target examines the information provided by the social engineer [118]. Target' ability to evaluate information initially depends on their personality traits [10, 49, 92, 123, 124, 154, 193] because specific personality traits favour more efficient cognitive abilities which lead to make a systematic evaluation, while others favour heuristic evaluation [141, 190] which is more favourable to social engineers. Another factor impacting the target's ability to evaluate is the target's knowledge broadly related to IT [7, 10, 78, 92, 123, 165]. It is one of the most studied user related characteristics for predicting the susceptibility of falling for phishing [198].

Of course the ability to evaluate is strongly determined by variables specific to each individual, but it is possible for a social engineer to use techniques to mitigate the beneficial effects of the target's skills and knowledge by distracting the target for example.

3.2.1 Time Pressure. The *Time Pressure* technique interferes with the target's attentional capacity by manipulating the fear of missing out on an impending deadline. Imposing strict time constraints on a request creates a sense of rarity, requiring quick action to seize the opportunity [1, 91]. This technique shortens the decision time of the target, decreasing cognitive abilities [72] and increase persuasiveness[11, 156].

3.2.2 Humour. The *Humour* technique is used in less than 8.77% of phishing emails [91]. However, humor can increase sales and reduce message comprehension [46], potentially making it more difficult to identify the authentic request of the social engineer. The use of humor can distract the target's attention and direct their cognitive focus towards interpreting the content as a joke, distracting from the primary intent of the social engineering message.

3.2.3 Parallel Tasking. The *Parallel Tasking* technique affects the target's attention span by distracting them with an additional task during the actual task presentation [11, 156]. Moreover, a distracted target produced fewer counterarguments and were more likely to stick with the presented argument [139]. This technique can be used in social engineering to encourage the target to focus on the extra task, compromising their critical thinking.

Table 1. Motivation to Evaluate: Examples

Manipulation technique	Example
Reciprocity	"Your welcome pack worth \$101 will arrive within 1 week." [The social engineer offers a \$100 welcome pack, exploiting the target's sense of obligation]
Fake consistency	"RE: Would you like to take out a loan to finance a project? The answer is here!" [Using a deceptive "RE:" in the message, the social engineer tricks the target into thinking they had a prior commitment, making them more likely to engage with a fraudulent loan offer]
Flattery	"Few people have managed to tackle the subject with such relevance."
Foot in the door	"Please tell me your email address." ; [...]; "Please tell me your address."
Door in the face	"I need €1,000 ; "No." ; "Please, at least 100€."
Scarcity	"Only 3 people have this NFT."
Request for Minor Favours	"What is your job ?"
Curiosity Appeal	"Elon_Musk_Suspected_of_Murder.pdf"
Reverse Psychology	"Do not click here."
Threatening	"Your computer has been encrypted, please send 10 bitcoin to avoid losing definitively all your data."
Humanitarianism	"If you don't send this transfer order, I'm going to loose my job."
Provocation	"You're not capable of taking any decisions without your boss."
Indignation	"This person doesn't pay his tax."
Baiting	"You have won \$1 million."
Disgust calling	"Buy our dietary supplement to avoid looking like this:" (disgusting picture attached)
Shameful disclosure	"Your Internet history contains porn searches."
Guilt Calling	"You did not answer me despite my multiple messages."
Social Pressure	"You are the last person in the company not to have installed the software."
Imply	"Your problem is solvable if you put some effort in it." [By hinting that effort can resolve the issue, the social engineer encourages the target to act accordingly]

3.2.4 Either-or Fallacy. The *Either-or Fallacy* affects the target's attention span by creating a distraction [11, 156]. It is a common rhetorical manipulation technique [178], presenting the target with two opposing options, each with different implications. The effectiveness of this technique was demonstrated by a study that introduced a non-dichotomous answer to an MCQ and observed a significant drop in the pass rate [140]. This is because human cognition tends to favour a limited number of options, which Kruglanski [98] refers to as the cognitive process of *cognitive closure*. False dichotomy is often used in disinformation to present false or misleading arguments by reducing the target's options to a binary choice, so that the target does not realize that the number of possible options is greater than what is being presented to them [155].

3.2.5 Hyperchleuasm. The *Hyperchleuasm* technique used by social engineers involves explicit truth or exaggerated version description, using irony [153]. This technique is similar to McGuire's inoculation [116], which aims to protect the target from an idea by suggesting the opposite idea. For example, a social engineer can inoculate bad security practices by suggesting an absurd pro-security idea, limiting their neutral reasoning ability : "Your computer will explode if you click on an unknown link". By doing so, the target's ability for neutral reasoning is limited.

3.2.6 Group Thinking. The *Group Thinking* technique aims to influence a person’s decision-making process through group viewpoints, based on the hypothesis that group members have a strong urge to achieve consensus and suppress dissenting opinions [6, 111]. Groupthink occurs when alternatives to the majority-shared option are not adequately expressed, leading to suboptimal decision-making that may be hazardous [81]. This technique differs from social pressure, because the target must be in real-time contact with a group which threaten the target social identity [172].

3.2.7 Threatening. (Double impact technique) This technique, presented in 2.1.10, can modify the target’s motivation and affect their message processing due to the strong emotional state of fear. Emotions, particularly negative ones, decrease logical thinking [85].

3.2.8 Provocation. (Double impact technique) The technique in Section 3.1.12, impacting the target’s motivation through anger, decrease attention towards elements other than the anger source [102], making social engineering attacks harder to identify. Anger can also reduce logical reasoning [85].

3.2.9 Baiting. (Double impact technique) The technique in Section 3.1.14 impacting the target’s motivation through envy can reduce logical reasoning [85]. Erotic baiting’s suggestive behaviours can lead to risky actions [166].

3.2.10 Disgust Calling. (Double impact technique) The technique in Section 3.1.15 impacting the target’s motivation through disgust can impair their cognitive abilities if the disgust-inducing object relates to their phobia, reducing their logical reasoning skills below average [85]. A social engineer could show spider images to an arachnophobe to temporarily impair their cognitive abilities.

3.2.11 Metaphor. The *Metaphor* technique uses figurative expressions to guide the target’s thinking towards a specific interpretation and away from others [175]. Targets influenced by metaphors attribute their opinion shifts to inherent motivations, not recognizing the metaphor as the cause [175]. For instance, a phishing scheme might use figurative language to deceive the victim into thinking they face a risk or have an exceptional opportunity, like comparing a password change to a road collision.

Table 2. Ability to Evaluate: Examples

Manipulation technique	Example
Time Pressure	<i>"Your account will be deleted in 24 hours!"</i>
Humour	<i>"There are only 10 types of human on the planet. Those who understand binary and those who don't."</i>
Parallel Tasking	<i>"Take a sheet of paper to write down what I tell you"; "Enter your password on the page in front of you".</i> [In a phone call, the social engineer instructs the target to both take notes and enter a password simultaneously.]
Either-or fallacy	<i>"You can either pay the fine now or later."</i> [Creates a false dilemma, showing only option about paying without considering other options]
Hyperchleuasm	<i>"This is a very dangerous virus."</i> [Exaggeration of the threat by saying that the virus is very dangerous when in fact it is]
Group Thinking	<i>"I'm sending you all the registration link, let's sign up now together." (in a visio)</i>
Metaphor	<i>"Investing your money with us is like buying a goose that lays golden eggs."</i>

3.3 Heuristic Evaluation

Heuristic evaluation is the use of mental shortcuts to make decisions about complex information [28, 86, 147]. Kahneman [86] highlight that these heuristics generate superficial and simplistic evaluations, neglecting relevant dimensions of the information. Social engineers can exploit the target's cognitive shortcuts by creating simple trust indicators [118, 148, 182]. The target will rely on these indicators, which serve as mental shortcuts, and build their entire perception around the rules that the social engineer has distorted. The techniques of manipulation used at this stage allow the social engineer to alter the evaluation of the message by introducing or eliminating cues used by the target.

3.3.1 Similarity. Social engineer creates a fake image and establishes shared characteristics with the target, leveraging causal attribution theory [70] and the relationship between trust and similarity [30, 39], including in virtual contexts [32]. Similarity also affects moral perception [4, 24] and establishes commonalities without revealing physical identity. The social engineer can generate a profile similar to the target using AI.

3.3.2 Include Half-confidential Detail. The addition of semi-confidential information creates a sense of proximity and eventually establishes a recurring relationship [122]. The information provided should be kept private and confidential, but it can also be specific enough to be tailored for the target audience, yet generic enough to be applicable to everyone, which is known as Barnum effect [51, 136]. This method is typical of spear-phishing attacks [8, 23], which aim at particular individuals by utilizing personal information to establish a sense of trust [73]. This technique is also efficient in marketing [30] as targeted ads augment sales by 30% [114].

3.3.3 Attractiveness. Evaluation of trust towards a person can be formed in just 100 milliseconds based on their physical appearance [187]. Physical attractiveness impacts perceived behaviour [30, 121]. This technique utilizes the correlation between social perception and causality, consistent with Heider's causal attribution theory [70]. Attributions of causes foster a constructive perception and increase the likelihood of favourable outcomes.

3.3.4 Authority. *Authority* technique enhances information credibility by suggesting the source is reliable, competent, or legitimate [75, 117]. Visual markers of authority, such as a suit and tie, drastically increase compliance [30]. Authority, as shown in Milgram's obedience study [119], can lead to extreme compliance to authority figures. Social engineers can exploit this by posing as authority figures.

3.3.5 Contact Data Present. This technique of manipulation involves incorporating contact information into the message sent by a social engineer [91]. It is used in 3.86% of attacks via provision of telephone information and 2.46% for email addresses [91]. The social engineer simply discloses contact information to the target, as its presence is significant, not its authenticity [91]. A marketing study [35] revealed that consumers consider contact data as part of a site's market orientation metric, positively associated with trustworthiness. Presence of contact data can create a favourable impression of the message sender as a professional, transparent, and customer-centric entity. This may impact the recipient's interpretation of other communication elements, such as information conveyed, reliability [75], and importance.

3.3.6 Semantic Attack. One hallmark of phishing is identity theft [122]. This concept, known as *Semantic Attack* [69], is the most prevalent approach in several models and taxonomies [15, 43, 50, 69, 79, 131, 154, 174]. URLs visually similar to authentic ones deceive up to 91% of users [41]. Email prefix spoofing has a 76.49% usage rate in the wild, while domain name spoofing has a 71.23% usage rate [91]. Identity spoofs on social networks may not necessarily belong to

known individuals; a large number are of unknown random users [57]. Social engineers can also spoof software GUI or Wi-Fi access point names to harvest identifiers or run malware [69].

3.3.7 Secure Communication Channel. The *Secure Communication Channel* technique involves contacting the target via a channel it considers secure [41, 122]. The appearance of a green padlock in the browser indicates secure communication, but it can create an illusion of sender identity and content integrity for users who lack expertise [41]. Social engineers select channels regarded as safe by the target audience, such as phishing, smishing, and vishing, which depend on whether the message is delivered through email, SMS, or voice call [79]. Users are more susceptible to being deceived via SMS or voice calls, as these channels are less prone to attacks compared to emails. Social engineers can easily spoof or impersonate indicators to manipulate users' trust.

3.3.8 Social pressure. (Double impact technique) This technique, presented in Section 3.1.18, modifies the target's motivation to evaluate and also alter heuristic evaluation of a message [30]. This technique also referred to as *Social proof* increases an object's perceived value by demonstrating its value to other individuals [30]. In social engineering, this technique can persuade a target to undertake a specific action by presenting evidence that other individuals have already performed the same action and attained a positive outcome, even if they are fictitious [83].

3.3.9 Use of Statistics. The *Use of Statistics* technique involves presenting numerical data to sway the target's opinion or behaviour [3, 195]. Statistical evidence and numerical claims can enhance message persuasiveness [3]. Numbers can provide targets with a sense of certainty and objectivity [195].

3.3.10 Argumentative Mille-feuille. The technique of *Argumentative Mille-feuille* involves stacking a multitude of arguments, regardless of their quality, to sway the target's opinion and behaviour. The more arguments presented, the greater the persuasiveness of the message [146]. Social engineers may employ this tactic to inundate the target with extensive information, creating the impression of complexity, and forcing the target to conclude that "at least one of the arguments presented must be true" [42]. For instance, a disinformation campaign may involve several arguments targeted towards discrediting a source, without presenting concrete evidence.

3.3.11 Obscurantism. The practice of obfuscation involves the use of complicated jargon, often referred to as "bullshit" [52], to deceive or impress. Targets with low levels of verbal intelligence or cognitive ability are more susceptible [144]. Social engineers use this technique to promote unfounded concepts using technical or scientific terms. For example, a social engineer might use phrases like 'synergy', 'paradigm' or 'quantum' to create the impression of a pioneering, powerful or trustworthy person.

3.3.12 Impress Management. The *Impress Management* technique involves presenting oneself with traits like kindness, humility, or reliability to enhance the persuasive impact of arguments. Heuristic processing leads to higher persuasiveness for individuals displaying certain characteristics, such as expertise, attractiveness, or similarity because the target focuses more on source cues than message content during heuristic processing [28, 147]. Social engineers exploit this by displaying friendliness, helpfulness, or honesty.

3.3.13 Non-verbal Synchronicity. The method of *Non-verbal Synchronicity* involves using hand gestures to reinforce arguments, improving the receiver's comprehension and endorsement of the message [192]. Receivers of high-synchrony messages, those with synchronised kinetic cues, had superior recall and persuasion. Social engineers can use this

technique to enhance persuasive impact by incorporating gestures into their speech, such as a promotional video featuring an individual demonstrating a scam's benefits through timely gestures to bolster its persuasive force.

3.3.14 False Impartiality. The technique of *False Impartiality* manipulates victims by presenting as a neutral, disinterested interlocutor. Victims are more likely to believe and accept information or recommendations from impartial sources [2]. Social engineers exploit this by providing arguments and counterarguments, increasing persuasiveness. This approach has been used in social media by influencers encouraging followers to invest or back causes, and in consumer websites providing impartial-looking information or discussions [19, 171].

3.3.15 Fake Divergence. This technique makes the target think there's no agreement and different view on a topic where there is. It creates doubt and confusion by presenting the topic as debatable or unsure. Seeing various opinions makes people more open to changing their mind [103]. Social engineers use this to weaken the target's stance with weak or wrong arguments from different sources. For example, a false cybersecurity advice campaign might have conflicting facts to question trusted info.

Table 3. Heuristic Evaluation: Examples

Manipulation technique	Example
Similarity	"Hello fellow doctor."
Include half-confidential detail	"Since yesterday's work, I can no longer connect."
Attractiveness	Photo of an attractive person [This is an example of a sample linkedin profile that uses a photo of an attractive person. The goal is to make the profile appealing]
Authority	"According to article L-123 of the Penal Code, You have been sentenced by the inspector. Please open the attachment for more details."
Contact Data Present	"Call us on 012345." [Including contact details like 012345 in the message enhances the social engineer's credibility]
Semantic Attack	"contact@faacebook.com" instead of contact@facebook.com
Secure communication channel	"Your messages are end-to-end encrypted."
Use of statistics	"45% guaranteed return."
Argumentative mille feuille	"Fast payment ; Secured payment ; Indispensable product ; Satisfied or refunded."
Obscurantism	"Our software employs cutting-edge metaheuristics and deep learning methods to calibrate your system variables, such as virtual memory management, preemptive multitasking, write-back policy, and socket programming."
Impress Management	"I love helping people !"
Non-verbal synchronicity	Making gestures in a presentation
False impartiality	"I'm saying this for you, but I have nothing to gain from it."
Fake divergence	"It's still unclear whether this crypto money is a scam or not." [The social engineer will emphasize the fact that a fraudulent cryptocurrency is not officially declared as a scam, even if there are many cues that indicate this. Moreover, when a cryptocurrency is stated as a scam, most of the time, it's too late for the victim]

3.4 Systematic Evaluation

Systematic evaluation, conversely to heuristic evaluation, employs a more meticulous and rigorous scrutiny of the data, utilizing intricate benchmarks and acknowledging multiple pertinent aspects [28, 147]. Divergent from heuristic evaluation, systematic evaluation necessitates a greater investment of time, energy, and cognitive resources [28, 147]. Systematic evaluation requires examining sources, seeking additional evidence, weighing arguments for and against, and evaluating the pros and cons before reaching a decision or conclusion [86, 118]. In brief, a methodical evaluation of a social engineering tactic can greatly diminish its success probability [118].

3.5 Discussion

In the classification of manipulation techniques presented in this section, we did our best to carefully review the literature in social and cognitive psychology so that we can provide a classification as exhaustive as possible. As a consequence, some of these techniques may be quite obvious and already massively used by the social engineers, but others may sound more original and probably not yet used. That is exactly the point of this survey. The systematic review of the literature allowed us to bring to light some manipulation techniques that may not be used as for now, but that will probably be used in a near future, taking into account the constant increase in the sophistication of the manipulation techniques.

Figure 2 provides a historical perspective on the emergence of these manipulation techniques in the literature. However, it is crucial to recognize the limitations of 2, which relies on the first and last citations within a section of this paper, potentially omitting older or newer publications. Additionally, some subsections on techniques may not pertain to the techniques themselves, but to their most significant cognitive aspects (refer to 3.1.2). Despite this, the timeline demonstrates a notable dichotomy: as cybersecurity rapidly advances, the fundamental cognitive processes leveraged by social engineers stay notably unchanged. Human cognition, shaped by inherent biases, norms, needs, and emotional responses, (see next Section) doesn't update at the same pace as software or security protocols. This creates a persistent vulnerability, a stable target for attackers in the shifting sands of technological advancement. While techniques like social pressure and reciprocity have deep roots in social psychology, others, such as semantic attacks and exploiting secure communication channels, are simply modern adaptations of these fundamental principles to the online world. The timeline underscores the dynamic nature of social engineering, with attackers constantly refining their methods, but it simultaneously highlights the static nature of the human element, which persists as the weakest link. This reinforces the importance of understanding these cognitive processes, not just the technical aspects of cybersecurity, to develop truly effective countermeasures. Staying abreast of the latest research and trends in manipulation techniques is crucial for building defenses that address both the evolving digital landscape and the persistent vulnerabilities of human cognition.

4 COGNITIVE PROCESS CATEGORIES

In the previous section, we described each manipulation technique potentially used by social engineers. For each of these techniques, we reviewed studies that have explored—empirically or theoretically—the cognitive processes that may underline their effectiveness. The literature in social and cognitive psychology offers a rich array of theoretical frameworks for understanding behaviour and decision-making, including *cognitive biases*, *social norms*, *needs*, and *emotions*—each with varying classifications and potentially overlapping definitions [71]. These frameworks offer candidate cognitive processes that may explain how and why social engineering manipulations work. More specifically,

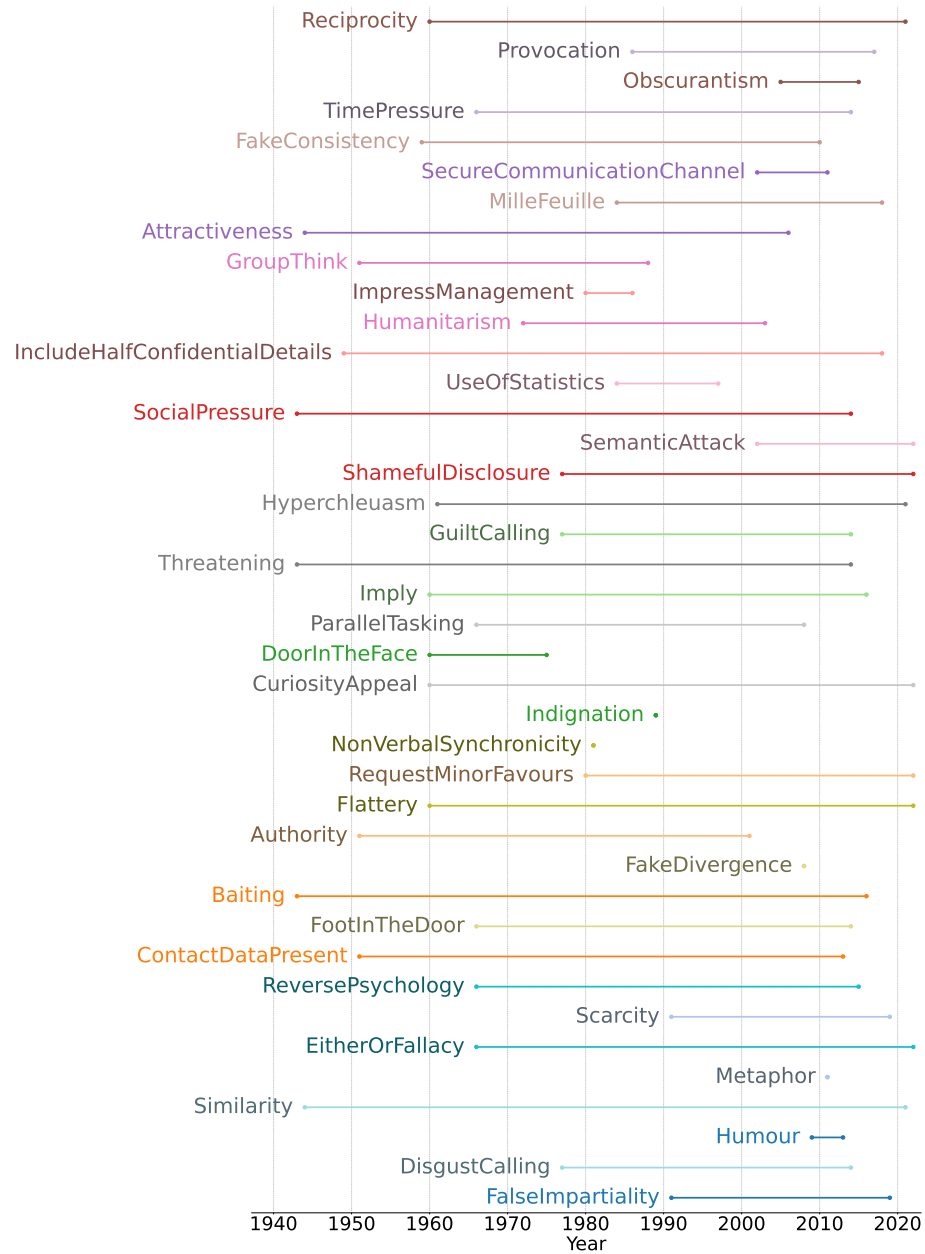


Fig. 2. Timeline of the emergence of manipulation techniques in the literature.

each theoretical framework provides a lens through which we can analyse the potential vulnerabilities exploited by different techniques. While there may be other relevant theoretical frameworks [201], we have chosen to focus on these four, drawing particularly on the work of Wen [184], who highlighted cognitive biases, needs, and emotions

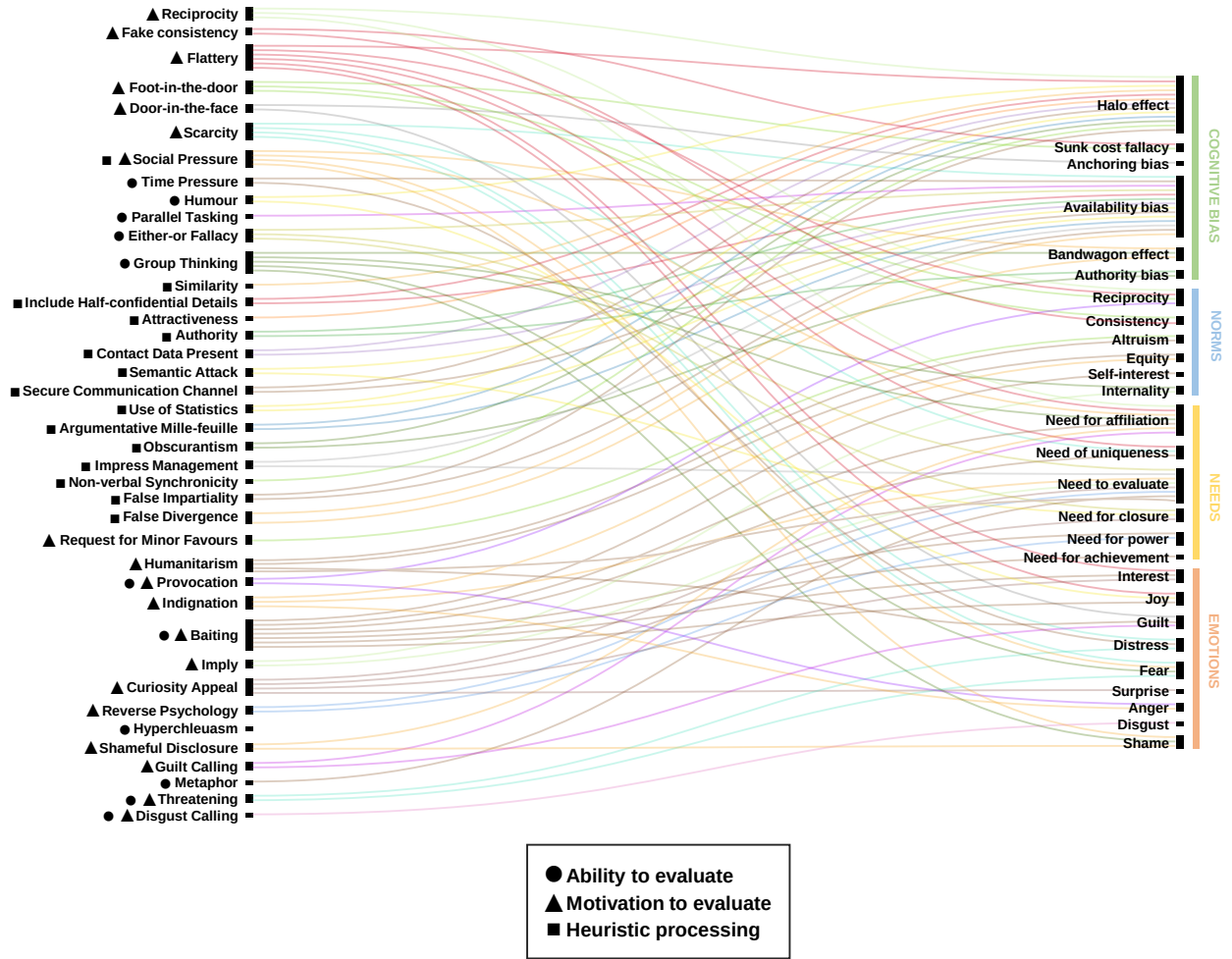


Fig. 3. Cognitive processes associated with manipulation technique.

as significant factors. We also incorporated *norms*, which we believe provide a more comprehensive perspective for understanding the range of cognitive processes potentially exploited by these techniques. In the following, we describe these theoretical frameworks, summarizing key definitions from the literature and suggesting which processes from each framework may be relevant to the manipulation techniques described earlier. Figure 3 provides a visual representation of the connections between each technique and the cognitive processes associated with each theoretical framework. Appendix A, B, C and D also represent these connections in tabular form (each table corresponds to one cognitive process). It is important to note that the connections shown in Figure 3 are based on our interpretation of existing literature and may not reflect the full complexity of these relationships. Further research is needed to empirically validate these connections and explore the interplay between different cognitive processes in the context of social engineering attacks.

4.1 Cognitive biases

Cognitive biases are systematic deviations of logical and rational thought from reality [86, 177]. Multiple cognitive biases influence everyday decisions, and unfortunately, behaviour on information systems is not exempt. To gain a better comprehension of the cognitive biases that social engineers can leverage, a short explanation aligned with each exploitable cognitive bias is as follows :

Halo effect : Overall evaluation based on a single salient or noticeable characteristic of an object or person [132]. For instance, if you think someone is attractive, you might rate their intelligence higher than it really is. An example would be rating an attractive professor as extremely intelligent and knowledgeable, even though you have no direct evidence for their intelligence, simply because of their overall positive qualities. A social engineer may take advantage of this cognitive bias by purposely highlighting some specific aspects of his personality, which may lead the victim to overestimate the social engineer and trust him.

Sunk cost fallacy : Irrational influence of an initial decision that influences future decisions in the same direction [151]. For instance, if you have committed a lot of resources to a project, you might be unwilling to abandon it even if it is not profitable or feasible. An example would be continuing to work on a project that has low chances of success, even though you have discovered a better opportunity, simply because of the resources you have already invested in the project. Even if this bias is quite specific (as can be seen in Appendix A), it can however be used by a social engineer in order notably to maintain the interaction with his victim.

Anchoring bias : Initial focus on a value that will serve as a reference point for future judgments and estimates [151]. For instance, if you are asked to estimate the value of a negotiation object, you might be influenced by the first offer that is made by the other party. An example would be accepting a higher price for a gas turbine than you would have otherwise, simply because the seller started with an inflated offer. This bias is also quite specific, but a social engineer may however take benefit of this bias by first asking something quite unreasonable to the victim and then by lowering his requirements, leading the victim to accept the demand.

Authority bias : Overvaluing the opinion of a person believed to have authority on a given subject [119]. For instance, if you are asked to evaluate the quality of a research paper, you might be influenced by the reputation or credentials of the author. An example would be rating a paper as highly original and rigorous, even though you have not read it carefully, simply because the author is a Nobel laureate or a professor at a prestigious university. A social engineer can take advantage of this bias by trying to convince the victim that he has authority over a specific subject, which may, in some scenarios, lead the victim to trust him.

Availability bias : Significant irrational influence of immediately available information in decision-making [176]. For instance, if you are asked to estimate the probability of a terrorist attack in your country, you might base your judgment on the vividness and recency of such events in your memory. An example would be overestimating the likelihood of a terrorist attack, even though the actual probability is very low, simply because of the salience and emotionality of the available information.

Bandwagon effect : Adoption of a behaviour through majority imitation [161]. For example, if you see that many people are buying a certain product, you might be more inclined to buy it yourself, even if you do not need it or know much about it. An example would be purchasing a popular smartphone model that has a high demand and positive reviews, without considering its features or alternatives. A social engineer may take advantage of this bias by trying to convince the victim to adopt a behaviour that is also adopted by a majority of persons, and then perceived as safe.

Appendix A illustrates the cognitive biases potentially exploited by each technique, based on our analysis of the literature. A checkmark (✓) indicates that the bias is likely exploited, while a question mark (?) suggests a possible connection that requires further investigation. This uncertainty reflects the limitations of existing research and the need for more empirical studies to confirm these relationships. Similar notation is used in subsequent tables regarding norms, needs, and emotions.

Cognitive biases are often employed in strategies that influence heuristic processing, aligning with current research on information processing [86, 118, 177, 184]. The *Halo Effect* appears to be a common tactic, potentially allowing social engineers to enhance their credibility by introducing irrelevant positive cues. This can be achieved directly, by emphasizing certain personality traits (*Reciprocity, Flattery, Humour, Similarity, Attractiveness, Impress Management, False Impartiality*), or indirectly, by embedding information within the message itself (*Include half-confidential details, Contact Data Present, Secure communication channel, Use of statistics, Argumentative mille feuille*). The *Obscurantism* technique may combine both approaches, using complex language to project an image of expertise. The role of the *Availability bias* in social engineering requires further exploration, as existing literature does not provide definitive evidence of its impact. The *Bandwagon effect* is clearly linked to social influence and is potentially relevant to techniques such as *Social Pressure, Group Thinking, and Fake divergence*. The remaining biases (*Authority, Sunk cost fallacy, Anchoring*) appear to be less prevalent, potentially due to their more specific nature and applicability to particular situations.

4.2 Norms

Norms are socially accepted rules or standards of behaviour that guide individuals' actions within a given group or community [150]. Social engineers may attempt to leverage these norms by appealing to individuals' desire to conform to social expectations. Conversely, social engineers may also exploit situations where adhering to a norm could lead to undesirable outcomes [150]. Here are some norms that attackers might exploit:

Norm of reciprocity : Social expectation that individuals will respond to each other in the same way, either through similar positive or negative actions [59]. An example would be accepting an invitation to a dinner party from a colleague who has previously given you some useful advice, without considering whether you really want to go or not. To exploit this norm, the social engineer must start by granting favours to a victim, who, in turn, should be more prone to realize actions that the social engineer suggests.

Norm of internality : Social expectation according to which an individual must explain events by causes inherent to himself rather than by external factors [13]. This cognitive process is also referenced by *Self-serving bias* [120] or *Fundamental attribution error* [157] in the psychology literature, with minor distinctions in this context. For example, if you are praised or blamed for something you did or something that happened to you, you might tend to attribute it to your own abilities, efforts, personality or intentions, rather than to external factors such as luck, chance, task difficulty or others' actions. This is because you feel that you are responsible for your own outcomes and that you have control over your own life. An example would be taking credit for getting a good grade on an exam because you studied hard and knew the material well, without considering the role of the teacher, the test difficulty or the grading system. To exploit this norm, the social engineer must convince the victim that the actions he's realizing can be attributed to his own abilities or personality, whereas these actions are in reality driven by the social engineer.

Norm of self-interest : Social expectation according to which an individual should not perform actions that are perceived as being against their interest [149]. For example, if you are faced with a choice between two social causes to support, such as environmental protection or animal rights, you might tend to favour the one that has more personal relevance or benefit for you, rather than the one that has more global or moral significance. This is because you

feel that you should act in accordance with your own interests and preferences, and that it would be irrational or wasteful to support a cause that does not affect you directly. An example would be choosing to donate money to a local environmental organization that works to improve the air quality in your city, without considering the plight of endangered animals in other parts of the world. To exploit this norm, the social engineer must persuade the victim that the actions he performs are in accordance with his own interests.

Norm of equity : Social expectation according to which goods should be fairly distributed [133]. For example, if you work on a group project with a partner who does less work than you, you might expect to receive a higher grade or a larger share of the credit than your partner. This is based on the norm of equity, which states that people should receive rewards or outcomes that are proportional to their inputs or contributions. An example would be trying to restore equity in an unfair situation which advantage a specific group of people and deserve another group. To exploit this norm, the victim must perceive the action demanded by the social engineer as an action which aims to maintain or restore equity between people in a situation.

Norm of altruism: Social expectation according to which an individual should help someone in need [17]. For example, if you see someone in distress or danger, you might feel compelled to help them, even if you do not know them or have any personal connection to them. You might risk your own safety or well-being, or sacrifice your time or resources, to assist them in their situation. An example would be trying to give money for an organisation even if you do not have the budget to do it. To exploit this norm, the social engineer must persuade the victim that the actions he performs are helpful for some other people and, as a consequence, that he is a good person. It is contrasted with self-interest norm, which is activated in different situations [87].

Norm of consistency : Social expectation according to which an individual should be consistent over time [64, 173]. This is the tendency to act in ways that are consistent with one's beliefs, values, and commitments. People who have a high preference for consistency are more likely to change their attitudes or behaviours to align with their prior actions or statements, especially when they are made salient or public. For example, if you have previously agreed to participate in a survey for a research project, you might be more likely to accept an invitation to join a focus group for the same project. This is because you want to act in ways that are consistent with your norm of consistency, which is your preference for behaving in accordance with your prior actions and statements. To exploit this norm, the social engineer must convince the victim that the actions he performs are in accordance with his prior actions and statements.

Appendix B shows the norms potentially exploited by each technique. The *reciprocity* norm appears most frequently, particularly in techniques influencing *motivation to evaluate* (*Reciprocity*, *Flattery*, *Foot in the door*, *Door in the face*, *Provocation*). This may be because reciprocity plays a key role in initiating and maintaining social interactions [59]. Other norms (*Internality*, *Self-interest*, *Equity*, *Altruism*, and *Consistency*) appear less frequently, possibly because they are more specific to certain situations. The relative absence of norms in techniques influencing heuristic processing may be due to the higher cognitive effort required to activate these norms, which may not be compatible with the rapid, less deliberative nature of heuristic processing.

4.3 Needs

In psychology, needs represent internal states that drive individuals to seek or achieve something [115]. Needs, as defined by McClelland as self-evaluated motives, can be influenced by external incentives, which social engineers might manipulate to achieve their goals. Here are some needs that attackers might exploit :

Need to evaluate: Need to assess and take a stance towards a situation [25, 82]. This is the tendency to form opinions about everything, regardless of whether it affects oneself or not. This need leads peoples to have strong and consistent

attitudes toward a variety of objects and issues, and to express them spontaneously. It is also this need which leads people to taking extreme positions, to not remain neutral, or to always have preference. An example would be having a strong opinion about a new movie that one has not seen. To exploit this need, the social engineer must place the victim in interaction with an attention grabber environment, such environment can be exposed to the victim through curiosity or outrageous news.

Need for closure: Need for reducing uncertainty and ambiguity [98, 130]. This creates an imperative to reach a clear and definite conclusion about something and to avoid any doubt or confusion. For example, people show tendencies towards urgency and permanence, meaning that they want to reach a fixed answer as quickly as possible and stick to it for a long time. They may also analyse information in a superficial and prejudiced manner, depending on initial cues, stereotypes, and consensus to reach a state of certitude faster. An example would be booking your flight and hotel as soon as possible and stick to your itinerary for the whole duration of your trip. To exploit this need, the social engineer must put the victim in an uncertain or ambiguous situation, forcing him to react, to take a quick and final decision.

Need for affiliation: Need to establish and maintain social relationships [95, 115]. Belonging to a social group, such as friends, neighbours and colleagues, is a natural outcome of the human need for affiliation. Furthermore, affiliation causes people to be sociable, friendly, and interested in social interactions, and they prefer to be with other people rather than alone. The need for affiliation also makes people seek out contact with others and to establish, maintain and re-establish positive relationships with them. For example, joining a club or team that shares their interests or hobbies, or seeking comfort and advice from a friend or family member. The social engineer can exploit this need by persuading the target that they share a common group identity or by inviting the target to join a new group, with the objective of establishing a positive relationship between them.

Need for power: Need to influence and affect others [115]. This need drives people to control or influence others, regardless of their actual power. This explains why people seek to be in charge, to make others follow their wishes, to earn respect and fame, to enjoy leading and deciding, to be less cooperative, less compliant, and more concerned with status or prestige. For instance, this behaviour may be observed in the context of organizing a protest march or participating in a debate club. In both instances, the individual would try to influence the outcome of the event, persuade others to follow their views, and gain recognition for their role. The social engineer exploits the target's need for leadership by persuading them that the requested tasks are opportunities for controlling and influencing others.

Need for achievement: Need to achieve significant goals [115]. This need makes people accomplish challenging goals, to master skills, and to excel in one's performance. This is the cause why people want to improve themselves, tend to set high standards for themselves and seek feedback on their progress, looking for tasks that are challenging. An example of the need for achievement would be studying hard for an exam, or preparing a presentation for a meeting. In both cases, the person wants to achieve a high score or positive feedback, to demonstrate to their self their competence. To exploit this need, the social engineer must persuade the victim that the actions he performs correspond to challenging tasks that prove his competence. It differs from the norm of internality because it pushes to the realisation of achievement and not identifying their cause like the norm of internality does. The social engineer exploits the target's need for achievement by making them believe that they are performing a difficult task that showcases their abilities.

Need for uniqueness: Need for feeling different and distinguishable from others [100]. Oppositely to need for affiliation, this need make people want to be different from others and to avoid conformity [74]. It also causes people to seek products and experiences that are rare, novel, or customized and avoid products and experiences that are common, popular, or standardized. An example would be if you are shopping for a new car, you might prefer a model that has a limited edition colour, a personalized licence plate, or a customized design. This way, you can express your individuality

and stand out from other car owners. The social engineer can exploit the target's need for uniqueness by inducing them to think that the actions they perform make them stand out.

As shown in Appendix C, needs appear less frequently in techniques influencing heuristic processing [184]. Many of the techniques that do exploit needs seem to target the *motivation to evaluate* and *ability to evaluate* phases. Needs may act as cognitive processes that direct individuals towards certain activities by offering a sense of satisfaction when fulfilled [115, 158]. This could potentially disrupt the evaluation of a message, leading to heuristic processing. The needs for affiliation and evaluation appear most frequently. The need for affiliation may be relevant to techniques involving interaction with real or fictitious groups (*shameful disclosure, social pressure, group thinking*) or where maintaining a positive relationship with the social engineer is important (*reciprocity, flattery, baiting, guilt calling*). The need to evaluate is also prevalent, possibly because it encourages individuals to explore their environment, which might be a precursor to aggressive behaviour. Aggression, in turn, has been linked to susceptibility to social engineering [66, 184, 191, 193]. The connection between a specific technique and the corresponding need can be complex. For example, in the *indignation* technique, the need to evaluate might be exploited because the source of indignation is external to the target [82]. In contrast, the *provocation* technique focuses on the target directly, which may not align with the need to evaluate.

4.4 Emotions

Emotions are complex reactions involving physiological changes, subjective experiences, and expressive behaviours, triggered by specific events or situations [138]. These reactions can influence an individual's tendency to approach or avoid a stimulus [80]. Social engineers may attempt to manipulate these approach and avoidance tendencies by evoking specific emotions, thereby influencing the target's attitudes, behaviours, and choices [135]. Triggering approach emotions might encourage action, while triggering avoidance emotions might discourage behaviours or choices that would otherwise raise suspicion.

Interest: The emotion of interest-excitement drives individuals towards a stimulus. This emotion has an evolutionary basis, as it has helped humans survive and reproduce by directing their actions towards beneficial outcomes. For example, when individuals come across a new and intriguing product, they might feel an emotion of interest-excitement, motivating them to explore and learn more about it. A social engineer can exploit this emotion by creating curiosity-inducing phishing emails or social media posts that entice individuals to click on malicious links or download malware.

Joy: The emotion of joy results from achieving a goal or satisfying a need. This emotion has an evolutionary basis, as it positively reinforces successful behaviour. For example, when individuals receive positive feedback or rewards for their accomplishments, they experience an emotion of joy. A social engineer can exploit this emotion by sending fake notifications of winning a contest or receiving a prize, which may prompt individuals to click on malicious links or disclose sensitive information.

Surprise: The emotion of surprise is a brief emotion that occurs when something unexpected happens, causing a temporary interruption of attention. This emotion has an evolutionary basis, as it enables individuals to react quickly and adapt to changes in the environment. For example, when individuals receive an unexpected gift or encounter an unexpected event, they experience an emotion of surprise. A social engineer can exploit this emotion by sending unexpected messages or notifications that create a sense of urgency or require immediate action, leading individuals to make impulsive and potentially harmful decisions.

Distress: The emotion of distress-anguish comes from pain, loss, or failure. This emotion has an evolutionary basis, as it alerts individuals to danger or damage and prompts them to seek support or help. For example, when individuals experience the loss of personal data, failure in achieving a task, or negative feedback, they feel an emotion

of distress-anguish. A social engineer can exploit this emotion by sending alarming messages or notifications that claim the individual's personal information or accounts have been compromised, leading them to provide sensitive information.

Anger: The emotion of anger occurs when individuals' goals or desires are blocked or threatened. This emotion has an evolutionary basis, as it prepares individuals to fight or defend themselves against obstacles or aggressors. For example, when individuals encounter unfair treatment, encounter technical difficulties, or become victims of cyberbullying, they feel an emotion of anger. A social engineer can exploit this emotion by sending provocative or offensive messages that trigger anger and prompt aggressive, impulsive or careless responses.

Disgust: The emotion of disgust involves a strong aversion or repulsion to something perceived as unpleasant, offensive, or contaminating. This emotion has an evolutionary basis, as it protects individuals from harmful or infectious substances or situations. For example, when individuals come across offensive or inappropriate content, encounter unethical behaviour, they feel an emotion of disgust. A social engineer can exploit this emotion by sending malicious content or messages that trigger feelings of disgust, leading individuals to turn away from a part of the message including the security clues.

Despise: The emotion of contempt involves a feeling of superiority or disdain towards someone or something considered unworthy or inferior. This emotion has an evolutionary basis, as it enables individuals to maintain their social status or prestige. For example, when individuals compare themselves to others, judge others' competence, or criticize others' choices, they feel an emotion of contempt. A social engineer can exploit this emotion by using social engineering techniques that make individuals feel superior or more knowledgeable, leading them to underestimate the social engineer's malicious behaviour.

Fear: The emotion of fear involves a feeling of danger or threat and a desire to escape or avoid it. This emotion has an evolutionary basis, as it prepares individuals to flee or hide from predators or enemies. For example, when individuals perceive potential risks or threats to their personal safety, privacy, or financial well-being, they feel an emotion of fear. It differs from distress, as distress is primarily triggered by negative events or outcomes and is associated with feelings of sadness or vulnerability, while fear is primarily triggered by perceived danger or threat and is associated with feelings of unease or heightened arousal. A social engineer can exploit this emotion by creating a sense of urgency or fear through phishing emails that claim the individual's accounts have been compromised or that their personal information is at risk, leading them to provide sensitive information.

Shame: The emotion of shame involves a feeling of exposure, humiliation, or inadequacy in relation to oneself or others. This emotion has an evolutionary basis, as it encourages individuals to respect social norms and avoid rejection or ostracism. For example, when individuals make mistakes, violate ethical rules, or experience public embarrassment, they feel an emotion of shame. A social engineer can exploit this emotion by using social engineering techniques that manipulate individuals into believing they have violated social norms or committed unethical actions, leading them to comply with the social engineer's requests.

Guilt: The emotion of guilt involves a feeling of responsibility or remorse for having done something wrong or having harmed someone else. This emotion has an evolutionary basis, as it motivates individuals to right their wrongs and maintain social relationships. For example, when individuals realize they have caused harm, deceived others or violated trust, they feel guilty. A social engineer can exploit this emotion by using guilt-inducing techniques, such as claiming that the individual's actions have led to negative consequences for others or that they are responsible for a security breach, leading them to comply with the social engineer's requests.

Based on our analysis shown in Appendix D, emotions appear to be frequently present in techniques that affect the *motivation to evaluate*, though more research is needed to confirm this pattern. This might suggest that strong emotional reactions could increase the likelihood of a target engaging with a message, potentially aligning with theories about approach and avoidance responses to emotions [80]. Some research indicates that emotions may facilitate rapid responses to external stimuli [55, 63, 80], possibly at the expense of logical reasoning [85]. In the context of social engineering, the message itself might act as the external stimulus, and the emotional response could potentially increase the target's motivation to process the message, though this relationship requires further investigation.

We did not find sufficient evidence in the literature suggesting a direct or indirect impact of *contempt* on persuasion, so it is not included in Appendix D. Some studies suggest that *fear* might be commonly exploited [91], potentially aligning with research by Witte [188] suggesting its persuasive effectiveness. However, it's important to note that while fear may be frequently exploited, it may not necessarily be the most prevalent emotion across all manipulation techniques. *Surprise* and *disgust* appear less frequently in our analysis, possibly because, as potential avoidance emotions [55, 138], their overuse might demotivate the target from engaging with the message, though this hypothesis requires further testing.

4.5 Discussion

Our preliminary analysis of these theoretical frameworks suggests that cognitive biases and needs might play important roles in many social engineering manipulation techniques, though the exact nature and extent of their influence remain to be fully understood. Cognitive biases appear to be particularly relevant to techniques that could encourage heuristic processing, while needs might be more influential in techniques that potentially affect motivation to evaluate.

The relationship between manipulation techniques and cognitive processes appears to be quite complex, and in many cases, the connections we have proposed would benefit from further empirical validation. For instance, while we can hypothesize about how certain techniques might exploit specific cognitive biases or needs, the actual mechanisms through which these processes operate in social engineering contexts remain somewhat unclear. Future research, particularly involving analysis of large corpora of social engineering communications, could help to validate or refine these proposed connections.

It seems important to note the diversity and sometimes contrasting nature of the cognitive processes that might be involved. For example, the need for uniqueness and the need for affiliation appear to represent opposing motivations, suggesting that different techniques might work through different - and sometimes competing - psychological mechanisms. But, in many cases, particularly in large-scale phishing campaigns, the attacker cannot know the specific cognitive processes that might drive each individual target's response. As a consequence, he might use a large set of manipulation techniques, even competing. On the other hand, in more targeted attacks, social engineers might attempt to profile their victims to identify potentially effective manipulation strategies and only use these strategies.

These observations suggest that understanding the range of cognitive processes that could potentially be exploited in social engineering attacks might be valuable for developing more effective countermeasures and educational interventions. However, much work remains to be done to fully understand these relationships and to develop evidence-based approaches to preventing social engineering attacks. The connections shown in Figure 3 should therefore be viewed as preliminary hypotheses rather than definitive relationships, and we encourage further research to test and refine these proposed connections.

5 CONCLUSION

In this survey, we have proposed a comprehensive study of manipulation techniques employed by the social engineers, by analysing the literature in social and cognitive psychology. In order to perform a relevant analysis, we have brought around the table scientists from the worlds of social/psychological science and computer science. Such a comprehensive study is quite difficult because social engineering represents a multifaceted challenge, relying on the manipulation of different cognitive processes that are not easy to classify.

After a short presentation of different representations of manipulation techniques as currently described in the cybersecurity literature, we have proposed a detailed list of the manipulation techniques that can be identified in the literature in social and cognitive psychology, along with simple examples that suggest how these manipulation techniques may be actually used in social engineering attacks. This classification is much richer than the classification in the cybersecurity literature, notably because it goes deeper in the analysis of the human cognitive processes that are employed in these techniques. These cognitive processes are presented and categorized into cognitive biases, norms, needs and emotions. Even if we are aware that the initial features of a target have a significant impact on the likelihood of falling for social engineering attacks (possibly until 69% as presented in [159]), we argue that the cognitive process involved in a social engineering attacks are really significant in the success of the attack, whoever the victim is, and that is it important to understand them.

This survey can be useful for different future works. Indeed, the different research works in social psychology that we studied for this survey also propose some specific countermeasures to the negative effects of the cognitive biases [37, 94], norms [6, 109], needs [163] and emotions [16, 63]. Even though these countermeasures are not specifically proposed in a cybersecurity context, they can be carefully analysed and adapted to the specific cybersecurity use case so that we can propose appropriate countermeasures and adapted awareness sessions against social engineering attacks. Even if technological safeguards remain indispensable in the defense against social engineering, the synergy between psychological insights and technological solutions holds the key to establishing a robust defense in the ever-evolving landscape of cybersecurity. By doing so, we hope to provide a useful framework for future research and practice in the field of social engineering prevention and detection.

We are also currently working on collecting a corpus of social engineering attacks (mostly emails at the moment). We analyse this corpus to measure the percentage of the different manipulations techniques identified in this survey that are actually used by the social engineers. Such analyses could bring really meaningful information for the scientific community so that we can better understand the different manipulation techniques that are privileged by the different social engineers as for now and propose appropriate countermeasures. This research work is currently done in cooperation with industrial partners that want to run some massive awareness campaign towards their employees.

Finally, an interesting future work also concerns the labeling of this corpus of attacks, according to the manipulation techniques identified in this survey. This corpus of labeled attacks can be used to train some IA models that can be further integrated in anti-spam tools for instance, in order to improve their detection capability against a large panel of attacks.

ACKNOWLEDGMENTS

We would like to express our deepest gratitude to the Cybersecurity Institute of Occitanie (ICO) for their financial support. Their contribution has been instrumental in carrying out the research presented in this paper. LLM was utilized to translate and transform writing style of text.

REFERENCES

- [1] N. Akbar. 2014. Analysing Persuasion Principles in Phishing Emails. <http://essay.utwente.nl/66177/>
- [2] Mike Allen. 1991. Meta-analysis comparing the persuasiveness of one-sided and two-sided messages. *Western Journal of Speech Communication* 55, 4 (Dec. 1991), 390–404. <https://doi.org/10.1080/10570319109374395>
- [3] Mike Allen and Raymond W. Preiss. 1997. Comparing the persuasiveness of narrative and statistical evidence using meta-analysis. *Communication Research Reports* 14, 2 (March 1997), 125–131. <https://doi.org/10.1080/08824099709388654>
- [4] A.B. Anderson. 1975. Combined effects of interpersonal attraction and goal-path clarity on the cohesiveness of task oriented groups. *Journal of Personality and Social Psychology* 31, 1 (1975), 68–75. <https://doi.org/10.1037/h0076233>
- [5] I. Arroyabe, C.F.A. Arranz, M.F. Arroyabe, and J.C. Arroyabe. 2023. Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019. *Computers & Security* 124 (2023), 102954. <https://doi.org/10.1016/j.cose.2022.102954>
- [6] SE ASCH. 1951. *Effects of group pressure upon the modification and distortion of judgements*. Carnegie Press. 177–190 pages.
- [7] A.H. Asfoor, F.A. Rahim, and S. Yusof. 2020. In *IDENTIFYING FACTORS THAT INFLUENCE SECURITY BEHAVIORS RELATING TO PHISHING ATTACKS SUSCEPTIBILITY : A SYSTEMATIC LITERATURE*.
- [8] T. Bakhshi. 2017. Social engineering: Revisiting end-user awareness and susceptibility to classic attack vectors. In *13th International Conference on Emerging Technologies (ICET)*. 1–6. <https://doi.org/10.1109/ICET.2017.8281653>
- [9] T. Bakhshi, M. Papadaki, and S. Furnell. 2009. Social engineering: Assessing vulnerabilities in practice. *Information Management & Computer Security* 17, 1 (2009), 53–63. <https://doi.org/10.1108/09685220910944768>
- [10] S. Baki and R. Verma. 2021. Sixteen Years of Phishing User Studies: What Have We Learned? <https://doi.org/10.48550/arXiv.2109.04661> arXiv:2109.04661). arXiv..
- [11] J. Baron. 2008. *Thinking and deciding* (4th ed.). Cambridge University Press.
- [12] R.A. Baron. 1973. The “foot-in-the-door” phenomenon: Mediating effects of size of first request and sex of requester. *Bulletin of the Psychonomic Society* 2, 2 (1973), 113–114. <https://doi.org/10.3758/BF03327736>
- [13] J.E.-L. Beauvois and N. Dubois. 1988. The norm of internality in the explanation of psychological events. *European Journal of Social Psychology* 18, 4 (1988), 299–316. <https://doi.org/10.1002/ejsp.2420180402>
- [14] I. Becheur and P. Valette-Florence. 2014. The use of negative emotions in health communication messages: Study of the effects of fear, guilt, and shame. *Recherche et Applications En Marketing (English Edition)* 29, 4 (2014), 89–109. <https://doi.org/10.1177/2051570714552620>
- [15] A. Berady. 2022. *Comprendre les menaces sophistiquées: Intentions, moyens, manières et connaissances convergentes des adversaires*. CENTRALE-SUPÉLEC.
- [16] M. Berking and B. Whitley. 2014. The Adaptive Coping with Emotions Model (ACE Model). In *Affect Regulation Training*, M. Berking and B. Whitley (Eds.). Springer New York, 19–29. https://doi.org/10.1007/978-1-4939-1022-9_3
- [17] L. Berkowitz. 1972. Social Norms, Feelings, and Other Factors Affecting Helping and Altruism. In *Advances in Experimental Social Psychology*. Vol. 6. Elsevier, 63–108. [https://doi.org/10.1016/S0065-2601\(08\)60025-8](https://doi.org/10.1016/S0065-2601(08)60025-8)
- [18] Parth Bhatt, Edgar Toshiro Yano, and Per Gustavsson. 2014. Towards a Framework to Detect Multi-stage Advanced Persistent Threats Attacks. In *2014 IEEE 8th International Symposium on Service Oriented System Engineering*. IEEE, Oxford, United Kingdom, 390–395. <https://doi.org/10.1109/SOSE.2014.53>
- [19] B. Bickart and R.M. Schindler. 2001. Internet forums as influential sources of consumer information. *Journal of Interactive Marketing* 15, 3 (2001), 31–40. <https://doi.org/10.1002/dir.1014>
- [20] Cesar Bravo and Desilda Toska. 2023. *The art of social engineering: uncover the secrets behind the human dynamics in cybersecurity* (1st edition ed.). Packt Publishing, Birmingham.
- [21] J.W. Brehm. 1966. *A theory of psychological reactance*. Academic Press. , pages.
- [22] D.M. Buss, M. Gomes, D.S. Higgins, and K. Lauterbach. 1987. Tactics of manipulation. *Journal of Personality and Social Psychology* 52, 6 (1987), 1219–1229. <https://doi.org/10.1037/0022-3514.52.6.1219>
- [23] M. Butavicius, K. Parsons, M. Pattinson, and A. McCormac. 2016. Breaching the Human Firewall: Social engineering in Phishing and Spear-Phishing Emails. <https://doi.org/10.48550/ARXIV.1606.00887>
- [24] D. Byrne. 1997. An Overview (and Underview) of Research and Theory within the Attraction Paradigm. *Journal of Social and Personal Relationships* 14, 3 (1997), 417–431. <https://doi.org/10.1177/0265407597143008>
- [25] J.T. Cacioppo and R.E. Petty. 1982. The need for cognition. *Journal of Personality and Social Psychology* 42, 1 (1982), 116–131. <https://doi.org/10.1037/0022-3514.42.1.116>

- [26] Deanna D. Caputo, Shari Lawrence Pfleeger, Jesse D. Freeman, and M. Eric Johnson. 2014. Going Spear Phishing: Exploring Embedded Training and Awareness. *IEEE Security & Privacy* 12, 1 (Jan. 2014), 28–38. <https://doi.org/10.1109/MSP.2013.106>
- [27] K.M. Carley. 2020. Social cybersecurity: An emerging science. *Computational and Mathematical Organization Theory* 26, 4 (2020), 365–381. <https://doi.org/10.1007/s10588-020-09322-9>
- [28] S. Chaiken. 1980. Heuristic versus systematic information processing and the use of source versus message cues in persuasion. *Journal of Personality and Social Psychology* 39, 5 (1980), 752–766. <https://doi.org/10.1037/0022-3514.39.5.752>
- [29] E. Chan and J. Sengupta. 2010. Insincere Flattery Actually Works: A Dual Attitudes Perspective. *Journal of Marketing Research* 47, 1 (2010), 122–133. <https://doi.org/10.1509/jmkr.47.1.122>
- [30] R.B. Cialdini. 2001. The Science of Persuasion. *Scientific American* 284, 2 (2001), 76–81.
- [31] R.B. Cialdini, J.E. Vincent, S.K. Lewis, J. Catalan, D. Wheeler, and B.L. Darby. 1975. Reciprocal Concessions Procedure for Inducing Compliance: The Door-in-the-Face Technique. *Journal of Personality and Social Psychology* 31 (1975), 206–215.
- [32] A.S. Clerke and E.A. Heerey. 2021. The Influence of Similarity and Mimicry on Decisions to Trust. *Collabra: Psychology* 7, 1 (2021), 23441. <https://doi.org/10.1525/collabra.23441>
- [33] G. Cluley. 2011. A 419 scam via snail mail. <https://nakedsecurity.sophos.com/2011/05/30/a-419-scam-via-snail-mail/> Naked Security..
- [34] F. Cohen. 2003. Internet Fraud. *Computer Fraud & Security* 2003, 4 (2003), 19. [https://doi.org/10.1016/S1361-3723\(03\)04013-2](https://doi.org/10.1016/S1361-3723(03)04013-2)
- [35] B.J. Corbitt, T. Thanasankit, and H. Yi. 2003. Trust and e-commerce: A study of consumer perceptions. *Electronic Commerce Research and Applications* 2, 3 (2003), 203–215. [https://doi.org/10.1016/S1567-4223\(03\)00024-3](https://doi.org/10.1016/S1567-4223(03)00024-3)
- [36] The MITRE Corporation. 2023. MITRE ATT&CK®. <https://attack.mitre.org/>
- [37] P. Croskerry, G. Singhal, and S. Mamede. 2013. Cognitive debiasing 1: Origins of bias and theory of debiasing. *BMJ Quality & Safety* 22, Suppl 2 (2013), 58–64. <https://doi.org/10.1136/bmjqs-2012-001712>
- [38] V. Curtis, M. Barra, and R. Aunger. 2011. Disgust as an adaptive system for disease avoidance behaviour. *Philosophical Transactions: Biological Sciences* 366, 1563 (2011), 389–401.
- [39] L.M. DeBruine. 2002. Facial resemblance enhances trust. *Proceedings of the Royal Society of London. Series B: Biological Sciences* 269, 1498 (2002), 1307–1312. <https://doi.org/10.1098/rspb.2002.2034>
- [40] Innovation Technology Department for Science. 2023. Cyber security breaches survey 2023. <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023>
- [41] Rachna Dhamija, J. D. Tygar, and Marti Hearst. 2006. Why Phishing Works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Montréal, Québec, Canada) (CHI '06). Association for Computing Machinery, New York, NY, USA, 581–590. <https://doi.org/10.1145/1124772.1124861>
- [42] D. Dorsaz. 2018.
- [43] Julie S. Downs, Mandy B. Holbrook, and Lorrie Faith Cranor. 2006. Decision Strategies and Susceptibility to Phishing. In *Proceedings of the Second Symposium on Usable Privacy and Security* (Pittsburgh, Pennsylvania, USA) (SOUPS '06). Association for Computing Machinery, New York, NY, USA, 79–90. <https://doi.org/10.1145/1143120.1143131>
- [44] Charles E Drehmer. 2021. *Reciprocity: An Antecedent to Fraud Compliance and Unethical Behavior*. Ph. D. Dissertation. DePaul University.
- [45] M. Eddy and N. Perloth. 2020. Cyber Attack Suspected in German Woman's Death. <https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomware-death.html>.
- [46] M. Eisend. 2009. A meta-analysis of humor in advertising. *Journal of the Academy of Marketing Science* 37, 2 (2009), 191–203. <https://doi.org/10.1007/s11747-008-0096-y>
- [47] A. Ferreira, L. Coventry, and G. Lenzini. 2015. Principles of Persuasion in Social Engineering and Their Use in Phishing. In *Human Aspects of Information Security, Privacy, and Trust*, T. Tryfonas and I. Askoxylakis (Eds.). Springer International Publishing, 36–47. https://doi.org/10.1007/978-3-319-20376-8_4
- [48] L. Festinger and J.M. Carlsmith. 1959. Cognitive consequences of forced compliance. *The Journal of Abnormal and Social Psychology* 58, 2 (1959), 203–210. <https://doi.org/10.1037/h0041593>
- [49] P. Fischer, S.E.G. Lea, and K.M. Evans. 2013. Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of scam compliance: The psychology of scams. *Journal of Applied Social Psychology* 43, 10 (2013), 2060–2072. <https://doi.org/10.1111/jasp.12158>
- [50] C.F.M. Foozy, R. Ahmad, M.F. Abdullah, R. Yusof, and M.Z. Mas'ud. 2012. Generic Taxonomy of Social Engineering Attack and Defence Mechanism for Handheld Computer Study.
- [51] Bertram R. Forer. 1949. The fallacy of personal validation: a classroom demonstration of gullibility. *The Journal of Abnormal and Social Psychology* 44, 1 (Jan. 1949), 118–123. <https://doi.org/10.1037/h0059240>
- [52] H.G. Frankfurt. 2005. *On bullshit*. Princeton University Press.
- [53] J.L. Freedman and S.C. Fraser. 1966. Compliance without pressure: The foot-in-the-door technique. *Journal of Personality and Social Psychology* 4, 2 (1966), 195–202. <https://doi.org/10.1037/h0023552>
- [54] H.H. Friedman and P.J. Herskovitz. 1990. The Effect of a Gift-Upon-Entry on Sales: Reciprocity in a Retailing Context. *American Journal of Business* 5, 1 (1990), 49–50. <https://doi.org/10.1108/19355181199000006>
- [55] N.H. Frijda. 1986. *The Emotions*. Cambridge University Press.

- [56] Paul Giura and Wei Wang. 2012. A Context-Based Detection Framework for Advanced Persistent Threats. In *2012 International Conference on Cyber Security*. IEEE, Alexandria, VA, USA, 69–74. <https://doi.org/10.1109/CyberSecurity.2012.16>
- [57] Oana Goga, Giridhari Venkatadri, and Krishna P. Gummadi. 2015. The Doppelgänger Bot Attack: Exploring Identity Impersonation in Online Social Networks. In *Proceedings of the 2015 Internet Measurement Conference (Tokyo, Japan) (IMC '15)*. Association for Computing Machinery, New York, NY, USA, 141–153. <https://doi.org/10.1145/2815675.2815699>
- [58] R.A. Gordon. 1996. Impact of ingratiation on judgments and evaluations: A meta-analytic investigation. *Journal of Personality and Social Psychology* 71, 1 (1996), 54–70. <https://doi.org/10.1037/0022-3514.71.1.54>
- [59] A.W. Gouldner. 1960. The Norm of Reciprocity: A Preliminary Statement. *American Sociological Review* 25, 2 (1960), 161. <https://doi.org/10.2307/2092623>
- [60] D. Gragg. 2003. A Multi-Level Defense Against Social Engineering.
- [61] T. Greening. 1996. Ask and ye shall receive: A study in “social engineering”. *ACM SIGSAC Review* 14, 2 (1996), 8–14. <https://doi.org/10.1145/228292.228295>
- [62] T. Greitemeyer. 2022. Prosocial modeling: Person role models and the media. *Current Opinion in Psychology* 44 (2022), 135–139. <https://doi.org/10.1016/j.copsyc.2021.08.024>
- [63] J.J. Gross. 1998. The Emerging Field of Emotion Regulation. *An Integrative Review. Review of General Psychology* 2, 3 (1998), 271–299. <https://doi.org/10.1037/1089-2680.2.3.271>
- [64] R.E. Guadagno and R.B. Cialdini. 2010. Preference for consistency and social influence: A review of current research findings. *Social Influence* 5, 3 (2010), 152–163. <https://doi.org/10.1080/15534510903332378>
- [65] B.B. Gupta, N.A.G. Arachchilage, and K.E. Psannis. 2018. Defending against phishing attacks: Taxonomy of methods, current issues and future directions. *Telecommunication Systems* 67, 2 (2018), 247–267. <https://doi.org/10.1007/s11235-017-0334-z>
- [66] Lee Hadlington. 2017. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon* 3, 7 (2017), e00346. <https://doi.org/10.1016/j.heliyon.2017.e00346>
- [67] F. Hassandoust, H. Singh, and J. Williams. 2020. The Role of Contextualization in Individuals’ Vulnerability to Phishing Attempts. *Australasian Journal of Information Systems* 24 (2020). <https://doi.org/10.3127/ajis.v24i0.2693>
- [68] J.M. Hatfield. 2018. Social engineering in cybersecurity: The evolution of a concept. *Computers & Security* 73 (2018), 102–113. <https://doi.org/10.1016/j.cose.2017.10.008>
- [69] R. Heartfield and G. Loukas. 2015. A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks. *Comput. Surveys* 48, 3 (2015), 1–37 39. <https://doi.org/10.1145/2835375>
- [70] F. Heider. 1944. Social perception and phenomenal causality. *Psychological Review* 51, 6 (1944), 358–374. <https://doi.org/10.1037/h0055425>
- [71] M. Hilbert. 2012. Toward a synthesis of cognitive biases: How noisy information processing can bias human decision making. *Psychological Bulletin* 138, 2 (2012), 211–237. <https://doi.org/10.1037/a0025940>
- [72] R.M. Hogarth. 1975. Decision Time as a Function of Task Complexity. In *Utility, Probability, and Human Decision Making*, D. Wendt and C. Vlek (Eds.). Springer Netherlands, 321–338. https://doi.org/10.1007/978-94-010-1834-0_19
- [73] J. Hong. 2012. The state of phishing attacks. *Commun. ACM* 55, 1 (2012), 74–81. <https://doi.org/10.1145/2063176.2063197>
- [74] Matthew J. Hornsey and Jolanda Jetten. 2004. The Individual Within the Group: Balancing the Need to Belong With the Need to Be Different. *Personality and Social Psychology Review* 8, 3 (Aug. 2004), 248–264. https://doi.org/10.1207/s15327957pspr0803_2
- [75] C.I. Hovland and W. Weiss. 1951. The Influence of Source Credibility on Communication Effectiveness. *Public Opinion Quarterly* 15, 4 (1951), 635. <https://doi.org/10.1086/266350>
- [76] Daniel J. Howard. 1990. The Influence of Verbal Responses to Common Greetings on Compliance Behavior: The Foot-In-The-Mouth Effect. *Journal of Applied Social Psychology* 20, 14 (Aug. 1990), 1185–1196. <https://doi.org/10.1111/j.1559-1816.1990.tb00399.x>
- [77] Georgios Ioannou, Panos Louvieris, and Natalie Clewley. 2019. A Markov Multi-Phase Transferable Belief Model for Cyber Situational Awareness. *IEEE Access* 7 (2019), 39305–39320. <https://doi.org/10.1109/ACCESS.2019.2897923>
- [78] C. Iuga, J.R.C. Nurse, and A. Erola. 2016. Baiting the hook: Factors impacting susceptibility to phishing attacks. *Human-Centric Computing and Information Sciences* 6, 1 (2016), 8. <https://doi.org/10.1186/s13673-016-0065-2>
- [79] K. Ivaturi and L. Janczewski. 2011. A Taxonomy for Social Engineering attacks. <https://aisel.aisnet.org/confirm2011/15>.
- [80] C.E. Izard. 1977. *Human Emotions*. Springer US. <https://doi.org/10.1007/978-1-4899-2209-0>
- [81] I.L. Janis. 1972. *Victims of groupthink: A psychological study of foreign-policy decisions and fiascos*. Houghton Mifflin. , 277 pages.
- [82] W.B.G. Jarvis and R.E. Petty. 1996. The need to evaluate. *Journal of Personality and Social Psychology* 70, 1 (1996), 172–194. <https://doi.org/10.1037/0022-3514.70.1.172>
- [83] H. Jhaveri, H. Jhaveri, and D. Sanghavi. 2014. Sybil Attack and its Proposed Solution. *International Journal of Computer Applications* 105 (2014), 17–19.
- [84] H. Jung, E. Seo, E. Han, M.D. Henderson, and E.A. Patall. 2020. Prosocial modeling: A meta-analytic review and synthesis. *Psychological Bulletin* 146, 8 (2020), 635–663. <https://doi.org/10.1037/bul0000235>
- [85] N. Jung, C. Wrانke, K. Hamburger, and M. Knauff. 2014. How emotions affect logical reasoning: Evidence from experiments with mood-manipulated participants, spider phobics, and people with exam anxiety. *Frontiers in Psychology* 5 (2014). <https://doi.org/10.3389/fpsyg.2014.00570>
- [86] D. Kahneman. 2011. *Thinking, fast and slow* (1st ed.). Farrar, Straus and Giroux.

- [87] Olli E. Kangas. 1997. Self-interest and the common good: The impact of norms, selfishness and context in social policy opinions. *The Journal of Socio-Economics* 26, 5 (Jan. 1997), 475–494. [https://doi.org/10.1016/S1053-5357\(97\)90010-X](https://doi.org/10.1016/S1053-5357(97)90010-X)
- [88] A. Karakasiliotis, S. Furnell, and M. Papadaki. 2006. Assessing end-user awareness of social engineering and phishing. *Australian Information Warfare and Security Conference* (2006). <https://doi.org/10.4225/75/57a80e47aa0cb>
- [89] Hussein Khalifa Hassan Khalifa. 2022. A Conceptual Review on Heuristic Systematic Model in Mass Communication Studies. *International Journal of Media and Mass Communication* 04, 02 (July 2022). <https://doi.org/10.46988/IJMMC.04.02.2022.007>
- [90] C.A. Kiesler, S.B. Kiesler, and M.S. Pallak. 1967. The effect of commitment to future interaction on reactions to norm violations1. *Journal of Personality* 35, 4 (1967), 585–599. <https://doi.org/10.1111/j.1467-6494.1967.tb01450.x>
- [91] D. Kim and J. Hyun Kim. 2013. Understanding persuasive elements in phishing e-mails: A categorical content and semantic network analysis. *Online Information Review* 37, 6 (2013), 835–850. <https://doi.org/10.1108/OIR-03-2012-0037>
- [92] S. Kleitman, M.K.H. Law, and J. Kay. 2018. It's the deceiver and the receiver: Individual differences in phishing susceptibility and false positives with item profiling. *PLOS ONE* 13, 10 (2018), 0205089. <https://doi.org/10.1371/journal.pone.0205089>
- [93] U. Koch and K. Cratsley. 2020. Psychological Mechanisms. In *Encyclopedia of Personality and Individual Differences*, V. Zeigler-Hill and T.K. Shackelford (Eds.). Springer International Publishing, 4145–4154. https://doi.org/10.1007/978-3-319-24612-3_1562
- [94] Johan E. Korteling, G.L. Paradies, and J.P. Sassen-van Meer. 2023. Cognitive bias and how to improve sustainable decision making. *Frontiers in Psychology* 14 (2023), 1129835. <https://doi.org/10.3389/fpsyg.2023.1129835>
- [95] V.B. Kovač. 2016. *Affiliation Motivational System*. Palgrave Macmillan UK, 95–131 pages. https://doi.org/10.1057/978-1-137-47056-0_4
- [96] G. Krieg and T. Kopan. [n. d.]. *Is this the email that hacked John Podesta's account?* | CNN Politics. CNN. <https://www.cnn.com/2016/10/28/politics/phishing-email-hack-john-podesta-hillary-clinton-wikileaks/index.html>
- [97] K. Krombholz, H. Hobel, M. Huber, and E. Weippl. 2015. Advanced social engineering attacks. *Journal of Information Security and Applications* 22 (2015), 113–122. <https://doi.org/10.1016/j.jisa.2014.09.005>
- [98] A.W. Kruglanski and D.M. Webster. 1996. Motivated closing of the mind: “Seizing” and “freezing”. *Psychological Review* 103, 2 (1996), 263–283. <https://doi.org/10.1037/0033-295X.103.2.263>
- [99] K. Kryś, C. Xing, J.M. Zelenski, C.A. Capaldi, Z. Lin, and B. Wojciszke. 2017. Punches or punchlines? Honor, face, and dignity cultures encourage different reactions to provocation. *HUMOR* 30, 3 (2017). <https://doi.org/10.1515/humor-2016-0087>
- [100] F. Lalot, M. Cantarella, O. Zerhouni, E. Joly, A. Quiamzade, J.M. Falomir-Pichastor, O. Desrichard, and L. Bègue. 2019. Assessing private and public need for uniqueness: Validation of French Versions of the Need for Uniqueness (NFU) and Self-Attributed Need for Uniqueness (SANU) Scales. *Journal of Personality Assessment* 101, 3 (2019), 294–304. <https://doi.org/10.1080/00223891.2017.1394867>
- [101] J. Langenderfer and T.A. Shimp. 2001. Consumer vulnerability to scams, swindles, and fraud: A new theory of visceral influences on persuasion. *Psychology and Marketing* 18, 7 (2001), 763–783. <https://doi.org/10.1002/mar.1029>
- [102] J.S. Lerner and L.Z. Tiedens. 2006. Portrait of the angry decision maker: How appraisal tendencies shape anger's influence on cognition. *Journal of Behavioral Decision Making* 19, 2 (2006), 115–137. <https://doi.org/10.1002/bdm.515>
- [103] L.C. Levitan and P.S. Visser. 2008. The impact of the social context on resistance to persuasion: Effortful versus effortless responses to counter-attitudinal information. *Journal of Experimental Social Psychology* 44, 3 (2008), 640–649. <https://doi.org/10.1016/j.jesp.2007.03.004>
- [104] G. Loewenstein. 1994. The psychology of curiosity: A review and reinterpretation. *Psychological Bulletin* 116, 1 (1994), 75–98. <https://doi.org/10.1037/0033-2909.116.1.75>
- [105] G. Loewenstein and S. Issacharoff. 1994. Source dependence in the valuation of objects. *Journal of Behavioral Decision Making* 7, 3 (1994), 157–168. <https://doi.org/10.1002/bdm.3960070302>
- [106] E. Lombardi Vallauri. 2016. Implicits as Evolved Persuaders. In *Pragmemes and Theories of Language Use*, K. Allan, A. Capone, and I. Kecskes (Eds.). Vol. 9. Springer International Publishing, 725–748. https://doi.org/10.1007/978-3-319-43491-9_36
- [107] X. Luo, W. Zhang, S. Burd, and A. Seazzu. 2013. Investigating phishing victimization with the Heuristic–Systematic Model: A theoretical framework and an exploration. *Computers & Security* 38 (2013), 28–38. <https://doi.org/10.1016/j.cose.2012.12.003>
- [108] M. Lynn. 1991. Scarcity effects on value: A quantitative review of the commodity theory literature. *Psychology and Marketing* 8, 1 (1991), 43–57. <https://doi.org/10.1002/mar.4220080105>
- [109] J.-E. Lönnqvist, G. Walkowitz, P. Wichardt, M. Lindeman, and M. Verkasalo. 2009. The moderating effect of conformism values on the relations between other personal values, social norms, moral obligation, and single altruistic behaviours. *British Journal of Social Psychology* 48, 3 (2009), 525–546. <https://doi.org/10.1348/014466608X377396>
- [110] G. MacDonald, P.R. Nail, and J.R. Harper. 2011. Do people use reverse psychology? An exploration of strategic self-anticonformity. *Social Influence* 6, 1 (2011), 1–14. <https://doi.org/10.1080/15534510.2010.517282>
- [111] J.M. Marques, V.Y. Yzerbyt, and J.-P. Leyens. 1988. The “Black Sheep Effect”: Extremity of judgments towards ingroup members as a function of group identification. *European Journal of Social Psychology* 18, 1 (1988), 1–16. <https://doi.org/10.1002/ejsp.2420180102>
- [112] Lockheed Martin. 2011. Cyber Kill Chain®. <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>
- [113] A.H. Maslow. 1943. A theory of human motivation. *Psychological Review* 50 (1943), 370–396. <https://doi.org/10.1037/h0054346>
- [114] S.C. Matz, M. Kosinski, G. Nave, and D.J. Stillwell. 2017. Psychological targeting as an effective approach to digital mass persuasion. *Proceedings of the National Academy of Sciences* 114, 48 (2017), 12714–12719. <https://doi.org/10.1073/pnas.1710966114>

- [115] D.C. McClelland, R. Koestner, and J. Weinberger. 1989. How do self-attributed and implicit motives differ? *Psychological Review* 96, 4 (1989), 690–702. <https://doi.org/10.1037/0033-295X.96.4.690>
- [116] W.J. McGuire. 1961. Resistance to persuasion conferred by active and passive prior refutation of the same and alternative counterarguments. *The Journal of Abnormal and Social Psychology* 63, 2 (1961), 326–332. <https://doi.org/10.1037/h0048344>
- [117] D.H. McKnight and N.L. Chervany. 2001. What Trust Means in E-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology. *International Journal of Electronic Commerce* 6, 2 (2001), 35–59. <https://doi.org/10.1080/10864415.2001.11044235>
- [118] M.J. Metzger. 2007. Making sense of credibility on the Web: Models for evaluating online information and recommendations for future research. *Journal of the American Society for Information Science and Technology* 58, 13 (2007), 2078–2091. <https://doi.org/10.1002/asi.20672>
- [119] S. Milgram. 1974. Obedience to Authority: An Experimental View.
- [120] Dale T. Miller and Michael Ross. 1975. Self-serving biases in the attribution of causality: Fact or fiction? *Psychological Bulletin* 82, 2 (March 1975), 213–225. <https://doi.org/10.1037/h0076486>
- [121] P.R. Mims, J.J. Hartnett, and W.R. Nay. 1975. Interpersonal Attraction and Help Volunteering as a Function of Physical Attractiveness. *The Journal of Psychology* 89, 1 (1975), 125–131. <https://doi.org/10.1080/00223980.1975.9923913>
- [122] K.D. Mitnick and W.L. Simon. 2002. *The art of deception: Controlling the human element of security*. Wiley.
- [123] D. Modic and S.E.G. Lea. 2012. How Neurotic are Scam Victims, Really? The Big Five and Internet Scams. *SSRN Electronic Journal* (2012). <https://doi.org/10.2139/ssrn.2448130>
- [124] D. Modic and S.E.G. Lea. 2013. Scam Compliance and the Psychology of Persuasion. *SSRN Electronic Journal* (2013). <https://doi.org/10.2139/ssrn.2364464>
- [125] L. Montada and A. Schneider. 1989. Justice and emotional reactions to the disadvantaged. *Social Justice Research* 3, 4 (1989), 313–344. <https://doi.org/10.1007/BF01048081>
- [126] Rosana Montanez, Edward Golob, and Shouhuai Xu. 2020. Human Cognition Through the Lens of Social Engineering Cyberattacks. *Frontiers in Psychology* 11 (Sept. 2020), 1755. <https://doi.org/10.3389/fpsyg.2020.01755>
- [127] R. Montanez Rodriguez and S. Xu. 2022. Cyber Social Engineering Kill Chain. In *Science of Cyber Security*, C. Su, K. Sakurai, and F. Liu (Eds.). Vol. 13580. Springer International Publishing, 487–504. https://doi.org/10.1007/978-3-031-17551-0_32
- [128] B. Morenne. [n. d.]. Macron Hacking Attack: What We Know and Don't Know. <https://www.nytimes.com/2017/05/06/world/europe/emmanuel-macron-hacking-attack-what-we-know-and-dont-know.html>.
- [129] Nitin Naik, Paul Jenkins, Paul Grace, and Jingping Song. 2022. Comparing Attack Models for IT Systems: Lockheed Martin's Cyber Kill Chain, MITRE ATT&CK Framework and Diamond Model. In *2022 IEEE International Symposium on Systems Engineering (ISSE)*. 1–7. <https://doi.org/10.1109/ISSE54508.2022.10005490>
- [130] S.L. Neuberger and J.T. Newsom. 1993. Personal need for structure: Individual differences in the desire for simpler structure. *Journal of Personality and Social Psychology* 65, 1 (1993), 113–131. <https://doi.org/10.1037/0022-3514.65.1.113>
- [131] M. Nicho, H. Fakhry, and U. Egbue. 2018. Evaluating user vulnerabilities vs phisher skills in spear phishing. *IADIS INTERNATIONAL JOURNAL ON COMPUTER SCIENCE AND INFORMATION SYSTEMS* 13, 2 (2018), 93–108. https://doi.org/10.33965/ijcsis_2018130207
- [132] R.E. Nisbett and T.D. Wilson. 1977. The halo effect: Evidence for unconscious alteration of judgments. *Journal of Personality and Social Psychology* 35, 4 (1977), 250–256. <https://doi.org/10.1037/0022-3514.35.4.250>
- [133] M. Nishikawa and K. Hirata. 1978. THE EXPERIMENTAL INVESTIGATION OF EQUITY NORM UNDER INEQUITABLE DISTRIBUTION. *THE JAPANESE JOURNAL OF EXPERIMENTAL SOCIAL PSYCHOLOGY* 18, 1 (1978), 57–65. <https://doi.org/10.2130/jjesp.18.57>
- [134] Weina Niu, Xiaosong Zhan, Kenli Li, Guowu Yang, and Ruidong Chen. 2016. *Modeling Attack Process of Advanced Persistent Threat*. Lecture Notes in Computer Science, Vol. 10066. Springer International Publishing, Cham, 383–391. https://doi.org/10.1007/978-3-319-49148-6_32
- [135] G. Norris and A. Brookes. 2021. Personality, emotion and individual differences in response to online fraud. *Personality and Individual Differences* 169 (2021), 109847. <https://doi.org/10.1016/j.paid.2020.109847>
- [136] APA Dictionary of Psychology. 2018. Effect Barnum. <https://dictionary.apa.org/barnum-effect>
- [137] G.L. Orgill, G.W. Romney, M.G. Bailey, and P.M. Orgill. 2004. The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. In *Proceedings of the 5th Conference on Information Technology Education*. 177–181. <https://doi.org/10.1145/1029533.1029577>
- [138] A. Ortony and T.J. Turner. 1990. What's basic about basic emotions? *Psychological Review* 97, 3 (1990), 315. <https://doi.org/10.1037/0033-295x.97.3.315>
- [139] R.A. Osterhouse and T.C. Brock. 1970. Distraction increases yielding to propaganda by inhibiting counterarguing. *Journal of Personality and Social Psychology* 15, 4 (1970), 344–358. <https://doi.org/10.1037/h0029598>
- [140] M.V. Pachai, D. DiBattista, and J.A. Kim. 2015. A Systematic Assessment of 'None of the Above' on Multiple Choice Tests in a First Year Psychology Classroom. *The Canadian Journal for the Scholarship of Teaching and Learning* 6, 3 (2015). <https://doi.org/10.5206/cjsotl-rcacea.2015.3.2>
- [141] Rosemary Pacini and Seymour Epstein. 1999. The relation of rational and experiential information processing styles to personality, basic beliefs, and the ratio-bias phenomenon. *Journal of Personality and Social Psychology* 76, 6 (1999), 972–987. <https://doi.org/10.1037/0022-3514.76.6.972>
- [142] K. Parsons, A. McCormac, M. Pattinson, M. Butavicius, and C. Jerram. 2013. Phishing for the Truth: A Scenario-Based Experiment of Users' Behavioural Response to Emails. In *Security and Privacy Protection in Information Processing Systems*, L.J. Janczewski, H.B. Wolfe, and S. Shenoi (Eds.). Vol. 405. Springer, Berlin Heidelberg, 366–378. https://doi.org/10.1007/978-3-642-39218-4_27
- [143] T.R. Peltier. 2006. Social Engineering: Concepts and Solutions. *Information Systems Security* 15, 5 (2006), 13–21. <https://doi.org/10.1201/1086.1065898X/46353.15.4.20060901/95427.3>

- [144] G. Pennycook, J. Allan Cheyne, N. Barr, D.J. Koehler, and J.A. Fugelsang. 2015. On the reception and detection of pseudo-profound bullshit. *Judgment and Decision Making* 10, 6 (2015), 549–563. <https://doi.org/10.1017/S1930297500006999> Cambridge Core..
- [145] R.E. Petty and J.T. Cacioppo. 1979. Issue involvement can increase or decrease persuasion by enhancing message-relevant cognitive responses. *Journal of Personality and Social Psychology* 37, 10 (1979), 1915–1926. <https://doi.org/10.1037/0022-3514.37.10.1915>
- [146] R.E. Petty and J.T. Cacioppo. 1984. The effects of involvement on responses to argument quantity and quality: Central and peripheral routes to persuasion. *Journal of Personality and Social Psychology* 46, 1 (1984), 69–81. <https://doi.org/10.1037/0022-3514.46.1.69>
- [147] R.E. Petty and J.T. Cacioppo. 1986. *The Elaboration Likelihood Model of Persuasion*. Springer New York. 1–24 pages. https://doi.org/10.1007/978-1-4612-4964-1_1
- [148] K. Raman. 2008. Ask and you will receive. *McAfee Security Journal* (2008), 9–12.
- [149] R.K. Ratner and D.T. Miller. 2001. The norm of self-interest and its effects on social action. *Journal of Personality and Social Psychology* 81, 1 (2001), 5–16. <https://doi.org/10.1037/0022-3514.81.1.5>
- [150] K.J. Reynolds. 2019. Social norms and how they impact behaviour. *Nature Human Behaviour* 3, 1 (2019). <https://doi.org/10.1038/s41562-018-0498-x>
- [151] A. Rhode, A. Schönbohm, and J. Vliet. 2014. The tactical utilization of cognitive biases in negotiations. *Working Paper* (2014).
- [152] Nikki Robinson. 2023. HUMAN FACTORS SECURITY ENGINEERING: THE FUTURE OF CYBERSECURITY TEAMS. *EDPACS* 67, 5 (May 2023), 1–17. <https://doi.org/10.1080/07366981.2023.2211429>
- [153] J.-J. Robrieux. 2021. *Rhétorique et argumentation—4ed.* Armand Colin.
- [154] W. Rocha Flores, H. Holm, G. Svensson, and G. Ericsson. 2014. Using phishing experiments and scenario-based surveys to understand security behaviours in practice. *Information Management & Computer Security* 22, 4 (2014), 393–406. <https://doi.org/10.1108/IMCS-11-2013-0083>
- [155] J. Roozenbeek, S. Linden, B. Goldberg, S. Rathje, and S. Lewandowsky. 2022. Psychological inoculation improves resilience against misinformation on social media. *Science Advances* 8, 34 (2022), 6254. <https://doi.org/10.1126/sciadv.abo6254>
- [156] P.C. Rosenblatt. 1966. Persuasion as a function of varying amounts of distraction. *Psychonomic Science* 5, 2 (1966), 85–86. <https://doi.org/10.3758/BF03328292>
- [157] Lee Ross. 1977. *The Intuitive Psychologist And His Shortcomings: Distortions in the Attribution Process*. Vol. 10. Elsevier, 173–220. [https://doi.org/10.1016/S0065-2601\(08\)60357-3](https://doi.org/10.1016/S0065-2601(08)60357-3)
- [158] Robert Rybníček, Sabine Bergner, and Alfred Gutschelhofer. 2019. How individual needs influence motivation effects: a neuroscientific study on McClelland’s need theory. *Review of Managerial Science* 13, 2 (April 2019), 443–482. <https://doi.org/10.1007/s11846-017-0252-1>
- [159] D.M. Sarno, M.W. Harris, and J. Black. 2023. Which phish is captured in the net? Understanding phishing susceptibility and individual differences. *Applied Cognitive Psychology* 37, 4 (2023), 789–803. <https://doi.org/10.1002/acp.4075>
- [160] R. Schaumberg and S. Skowronek. 2022. Shame broadcasts social norms: The positive social effects of shame on norm acquisition and normative behavior. <https://doi.org/10.2139/ssrn.3792103> SSRN Scholarly Paper 3792103)..
- [161] R. Schmitt-Beck. 2015. Bandwagon Effect. In *The International Encyclopedia of Political Communication* (1st ed.), G. Mazzoleni (Ed.). Wiley, 1–5. <https://doi.org/10.1002/9781118541555.wbiepc015>
- [162] B. Schneier. 2015. *Secrets and lies: Digital security in a networked world*. John Wiley & Sons.
- [163] T. Scitovsky. 1992. *The Joyless Economy: The Psychology of Human Satisfaction*. Oxford University Press.
- [164] Y. Shang, K. Wang, Y. Tian, Y. Zhou, B. Ma, and S. Liu. 2023. Theoretical basis and occurrence of internet fraud victimisation: Based on two systems in decision-making and reasoning. *Frontiers in Psychology* 14 (2023), 1087463. <https://doi.org/10.3389/fpsyg.2023.1087463>
- [165] S. Sheng, M. Holbrook, P. Kumaraguru, L.F. Cranor, and J. Downs. 2010. Who falls for phish?: A demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 373–382. <https://doi.org/10.1145/1753326.1753383>
- [166] S. Skakoon-Sparling, K.M. Cramer, and P.A. Shuper. 2016. The Impact of Sexual Arousal on Sexual Risk-Taking and Decision-Making in Men and Women. *Archives of Sexual Behavior* 45, 1 (2016), 33–42. <https://doi.org/10.1007/s10508-015-0589-y>
- [167] Gunikhan Sonowal. 2023. *Social Engineering Attack: Rethinking Responsibilities and Solutions*. Nova Science Publishers. <https://doi.org/10.52305/KSOA7898>
- [168] Frank Stajano and Paul Wilson. 2011. Understanding scam victims: seven principles for systems security. *Commun. ACM* 54, 3 (March 2011), 70–75. <https://doi.org/10.1145/1897852.1897872>
- [169] S. Stasiukonis. 2006. *Social Engineering, the USB Way*. Dark Reading. <https://www.darkreading.com/perimeter/social-engineering-the-usb-way>
- [170] C. Steindl, E. Jonas, S. Sittenthaler, E. Traut-Mattausch, and J. Greenberg. 2015. Understanding psychological reactance: New developments and findings. *Zeitschrift Für Psychologie* 223, 4 (2015), 205–214. <https://doi.org/10.1027/2151-2604/a000222>
- [171] C. Stubb and J. Colliander. 2019. This is not sponsored content” – The effects of impartiality disclosure and e-commerce landing pages on consumer responses to social media influencer posts. *Computers in Human Behavior* 98 (2019), 210–222. <https://doi.org/10.1016/j.chb.2019.04.024>
- [172] Henri Tajfel and John C. Turner. 2004. *The Social Identity Theory of Intergroup Behavior* (0 ed.). Psychology Press, 276–293. <https://doi.org/10.4324/9780203505984-16>
- [173] B. Testé, S. Joffre, and A. Somat. 2010. L’expression de la préférence pour la consistance est-elle une norme de jugement comparable à l’expression de l’internalité ? *L’Année Psychologique* 110, 3 (2010), 401–425. <https://doi.org/10.3917/anpsy.103.0401>
- [174] P. Tetri and J. Vuorinen. 2013. Dissecting social engineering. *Behaviour & Information Technology* 32, 10 (2013), 1014–1023. <https://doi.org/10.1080/0144929X.2013.763860>

- [175] P.H. Thibodeau and L. Boroditsky. 2011. Metaphors We Think With: The Role of Metaphor in Reasoning. *PLoS ONE* 6, 2 (2011), 16782. <https://doi.org/10.1371/journal.pone.0016782>
- [176] A. Tversky and D. Kahneman. 1973. Availability: A heuristic for judging frequency and probability. *Cognitive Psychology* 5, 2 (1973), 207–232. [https://doi.org/10.1016/0010-0285\(73\)90033-9](https://doi.org/10.1016/0010-0285(73)90033-9)
- [177] A. Tversky and D. Kahneman. 1974. Judgment under Uncertainty: Heuristics and Biases: Biases in judgments reveal some heuristics of thinking under uncertainty. *Science* 185, 4157 (1974), 1124–1131. <https://doi.org/10.1126/science.185.4157.1124>
- [178] Fort Hays State University, J. Southworth, C. Swoyer, and University Oklahoma. 2020. *Critical Reasoning: A User's Manual*, v.4.0. Fort Hays State University. <https://doi.org/10.58809/QGVO1509>
- [179] Verizon. 2022. . DBIR Report 2022—Introduction. Verizon Business. <https://www.verizon.com/business/resources/reports/dbir/2022/introduction/>
- [180] A. Vishwanath, B. Harrison, and Y.J. Ng. 2018. Suspicion, Cognition, and Automaticity Model of Phishing Susceptibility. *Communication Research* 45, 8 (2018), 1146–1166. <https://doi.org/10.1177/0093650215627483>
- [181] R. Vonk. 2002. Self-serving interpretations of flattery: Why ingratiation works. *Journal of Personality and Social Psychology* 82, 4 (2002), 515–526. <https://doi.org/10.1037/0022-3514.82.4.515>
- [182] Z. Wang, H. Zhu, and L. Sun. 2021. Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods. *IEEE Access* 9 (2021), 11895–11910. <https://doi.org/10.1109/ACCESS.2021.3051633>
- [183] Rick Wash and Molly M. Cooper. 2018. Who Provides Phishing Training?: Facts, Stories, and People Like Me. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, Montreal QC Canada, 1–12. <https://doi.org/10.1145/3173574.3174066>
- [184] X. Wen, L. Xu, J. Wang, Y. Gao, J. Shi, K. Zhao, F. Tao, and X. Qian. 2022. Mental States: A Key Point in Scam Compliance and Warning Compliance in Real Life. *International Journal of Environmental Research and Public Health* 19, 14 (2022), 8294. <https://doi.org/10.3390/ijerph19148294>
- [185] G. White and J.H. Lee. 2021. *The Lazarus heist: How North Korea almost pulled off a billion-dollar hack*. BBC News. <https://www.bbc.com/news/stories-57520169>
- [186] M.T. Whitty and T. Buchanan. 2012. The Online Romance Scam: A Serious Cybercrime. *Cyberpsychology, Behavior, and Social Networking* 15, 3 (2012), 181–183. <https://doi.org/10.1089/cyber.2011.0352>
- [187] J. Willis and A. Todorov. 2006. First Impressions: Making Up Your Mind After a 100-Ms Exposure to a Face. *Psychological Science* 17, 7 (2006), 592–598. <https://doi.org/10.1111/j.1467-9280.2006.01750.x>
- [188] Kim Witte. 1994. Fear control and danger control: A test of the extended parallel process model (EPPM). *Communication Monographs* 61, 2 (June 1994), 113–134. <https://doi.org/10.1080/03637759409376328>
- [189] B. Wittes, C. Poplin, Q. Jurecic, and C. Spera. 2016. *Sextortion: Cybersecurity, teenagers, and remote sexual assault*. Center for Technology Innovation at Brookings. 1–47 pages.
- [190] Nicole L Wood. 2012. *Individual differences in decision-making styles as predictors of good decision making*. Ph. D. Dissertation. Bowling Green State University.
- [191] Stacey Wood, Pi-Ju Liu, Yaniv Hanoach, Patricia M. Xi, and Lukas Klapatch. 2018. Call to claim your prize: Perceived benefits and risk drive intention to comply in a mass marketing scam. *Journal of Experimental Psychology: Applied* 24, 2 (June 2018), 196–206. <https://doi.org/10.1037/xap0000167> 11 citations (Crossref) [2023-06-21].
- [192] W.G. Woodall and J.K. Burgoon. 1981. The effects of nonverbal synchrony on message comprehension and persuasiveness. *Journal of Nonverbal Behavior* 5, 4 (1981), 207–223. <https://doi.org/10.1007/BF00987460>
- [193] M. Workman. 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 (2008), 662–674. <https://doi.org/10.1002/asi.20779>
- [194] R.T. Wright, M.L. Jensen, J.B. Thatcher, M. Dinger, and K. Marett. 2014. Research Note—Influence Techniques in Phishing Attacks: An Examination of Vulnerability and Resistance. *Information Systems Research* 25, 2 (2014), 385–400. <https://doi.org/10.1287/isre.2014.0522>
- [195] Richard F. Yalch and Rebecca Elmore-Yalch. 1984. The Effect of Numbers on the Route to Persuasion. *Journal of Consumer Research* 11, 1 (June 1984), 522. <https://doi.org/10.1086/208988>
- [196] Y. Yi. 1990. Direct and indirect approaches to advertising persuasion. *Journal of Business Research* 20, 4 (1990), 279–291. [https://doi.org/10.1016/0148-2963\(90\)90007-Z](https://doi.org/10.1016/0148-2963(90)90007-Z)
- [197] C.M. Zedelius, M.E. Gross, and J.W. Schooler. 2022. Inquisitive but not discerning: Deprivation curiosity is associated with excessive openness to inaccurate information. *Journal of Research in Personality* 98 (2022), 104227. <https://doi.org/10.1016/j.jrp.2022.104227>
- [198] Sijie Zhuo, Robert Biddle, Yun Sing Koh, Danielle Lottridge, and Giovanni Russello. 2022. SoK: Human-Centered Phishing Susceptibility. arXiv:2202.07905 (Feb. 2022). <http://arxiv.org/abs/2202.07905> arXiv:2202.07905 [cs].
- [199] O. Zielinska, A. Welk, C.B. Mayhorn, and E. Murphy-Hill. 2016. The persuasive phish: Examining the social psychological principles hidden in phishing emails. In *Proceedings of the Symposium and Bootcamp on the Science of Security*. 126–126. <https://doi.org/10.1145/2898375.2898382>
- [200] P.G. Zimbardo. 1960. Involvement and communication discrepancy as determinants of opinion conformity. *The Journal of Abnormal and Social Psychology* 60, 1 (1960), 86–94. <https://doi.org/10.1037/h0040786>
- [201] . 2023. A Review of Telecom and Online Fraud Susceptibility Theories: A Psychological Perspective. *Advances in Psychology* 13, 10 (2023), 4389–4402. <https://doi.org/10.12677/AP.2023.1310553>

A COGNITIVE BIASES EXPLOITED BY MANIPULATION TECHNIQUES

	Cognitive bias					
	Halo effect	Sunk cost fallacy	Anchoring bias	Authority bias	Availability bias	Bandwagon effect
Motivation to Evaluate						
Reciprocity	✓					
Fake consistency		✓				
Flattery	✓					
Foot-in-the-door		✓				
Door-in-the-face			✓			
Scarcity					✓	
Request for Minor Favours						
Curiosity Appeal						
Reverse Psychology						
Threatening *						
Humanitarianism						
Provocation *						
Indignation *						
Baiting *						
Disgust Calling *						
Shameful Disclosure						
Guilt Calling						
Social Pressure *						✓
Imply						
Ability to Evaluate						
Time Pressure					✓	
Humour	✓					
Parallel Tasking					✓	
Either-or Fallacy					✓	
Hyperchleuasm						
Group Thinking						✓
Metaphor						
Heuristic Evaluation						
Similarity	✓					
Include Half-confidential Details	✓				✓	
Attractiveness	✓					
Authority				✓	?	
Contact Data Present	✓				?	
Semantic Attack					?	
Secure Communication Channel	✓				?	
Use of Statistics	✓				?	
Argumentative Mille-feuille	✓				✓	
Obscurantism	✓			✓		
Impress Management	✓				?	
Non-verbal Synchronicity	?					
False Impartiality	✓				?	
Fake Divergence					✓	✓

B NORMS EXPLOITED BY MANIPULATION TECHNIQUES

	Norms					
	Reciprocity	Internality	Self-interest	Equity	Altruism	Consistency
Motivation to Evaluate						
Reciprocity	✓					
Fake Consistency						✓
Flattery	✓					
Foot-in-the-door	✓					✓
Door-in-the-face	✓					
Scarcity						
Request for Minor Favours					✓	
Curiosity Appeal						
Reverse Psychology						
Threatening *						
Humanitarianism				✓	✓	
Provocation *	✓					
Indignation *				✓		
Baiting *			✓			
Disgust Calling *						
Shameful Disclosure						
Guilt Calling						
Social Pressure *						
Imply		✓				
Ability to Evaluate						
Time Pressure						
Humour						
Parallel Tasking						
Either-or Fallacy						
Hyperchleuasm						
Group Thinking		?				
Metaphor						
Heuristic Evaluation						
Similarity						
Include Half-confidential Details						
Attractiveness						
Authority						
Contact Data Present						
Semantic Attack						
Secure Communication Channel						
Use of Statistics						
Argumentative Mille-feuille						
Obscurantism						
Impress Management						
Non-verbal Synchronicity						
False Impartiality						
Fake Divergence						

C NEEDS EXPLOITED BY MANIPULATION TECHNIQUES

	Need for					
	Need to evaluate	Need for closure	Need for affiliation	Need for power	Need for achievement	Need of uniqueness
Motivation to Evaluate						
Reciprocity			✓			
Fake Consistency						
Flattery			✓			✓
Foot-in-the-door						
Door-in-the-face						
Scarcity						✓
Request for Minor Favours						
Curiosity Appeal	✓	✓				
Reverse Psychology	✓			?		
Threatening *						
Humanitarianism				✓		
Provocation *						
Indignation *	✓					
Baiting *			✓	✓	✓	✓
Disgust Calling *						
Shameful Disclosure			✓			
Guilt Calling			✓			
Social Pressure *			✓			
Imply	✓					
Ability to Evaluate						
Time Pressure						
Humour						
Parallel Tasking						
Either-or Fallacy	✓	✓				
Hyperchleuasm						
Group Thinking			✓			
Metaphor	✓					
Heuristic Evaluation						
Similarity						
Include Half-confidential Details						
Attractiveness						
Authority						
Contact Data Present						
Semantic Attack		✓				
Secure Communication Channel						
Use of Statistics						
Argumentative Mille-feuille						
Obscurantism						
Impress Management	✓					
Non-verbal Synchronicity						
False Impartiality						
Fake Divergence						

