Suspicious Minds: Psychological Techniques Correlated with Online Phishing Attacks

Ioannis Stylianou[a,b], Panagiotis Bountakas[a], Apostolis Zarras[a] and Christos Xenakis[a,b]

[a] University of Piraeus, Greece
[b] InQbit Innovations SRL, Romania

ARTICLE INFO

Keywords:
Cybersecurity
Social Engineering
Psychological Techniques
Behavioral Psychology
Persuasion
Compliance

ABSTRACT

Phishing remains a pervasive threat to information security, leveraging human psychology to manipulate individuals into disclosing sensitive information or performing actions against their best interests. This study presents a comprehensive taxonomy and analysis of psychological techniques utilized in social engineering, introducing novel metrics such as Absolute Compliance Increase Rate (ACR), Relative Compliance Increase Rate (RCR), and Comprehensive Compliance Increase Rate (CCR) to quantify their effectiveness. Our methodology involved a systematic review of existing literature and empirical data from psychological experiments to evaluate and compare the effectiveness of various techniques, including Authority, Commitment & Consistency, Reciprocity, and Group Pressure. The findings indicate that the Majority Size technique, measured by CCR, is particularly potent in scenarios with low initial compliance rates, while Authority, Commitment & Consistency, and Reciprocity also demonstrate high effectiveness. These insights enhance the understanding of the mechanics of social engineering techniques, enabling the development of more effective countermeasures against social engineering attacks.

1. Introduction

The digital age has made it increasingly easy for perpetrators to access vast amounts of information at their fingertips. Nevertheless, it is not the sheer volume of information and, frequently, neither the difficulty of implementing security countermeasures that pose the gravest threat; instead, it is the capacity to manipulate human perception which stands as a formidable challenge. The most notable social engineering attacks rely heavily on human psychology. As such, understanding the subtleties of human cognition becomes as essential as mastering the intricacies of the digital realm. It is one thing to crack a code or bypass a firewall, but convincing a human mind to willingly give up information is a testament to the potency of psychology in the hands of a skilled manipulator. However, while the threat remains considerable, the response is fragmented and often misdirected. The focus of most cybersecurity measures remains heavily skewed towards technology, often at the expense of understanding the human element. Thus, there is an urgent need to recalibrate this focus, blending technological fortifications with a deep dive into human psychology to better protect against emerging vulnerabilities.

This study marks a step toward that goal. Specifically, its primary objectives are to (*i*) develop a comprehensive taxonomy of techniques employed in phishing attacks, (*ii*) apply the newly proposed metrics introduced herein to quantify and compare the effectiveness of these techniques, and (*iii*) analyze their implementation in high-profile, real-world attacks.

Most decisions people make are handled by their unconscious, even more so in online contexts Newell and Shanks (2014); Muscanell, Guadagno and Murphy (2014). In this manuscript, we use the noun unconscious (and its adjectival counterpart nonconscious) to denote the automatic, System 1 mental processes that occur without deliberate awareness or intent Kahneman (2011); processes whose triggering stimuli are consciously perceived but whose influence on thought and behavior remains outside the individual's awareness Bargh and Morsella (2008). The nonconscious processes, being unable to be perceived and analyzed by definition, are susceptible to creating a false perception, therefore affecting the subject's decisions Steele and Morawski (2002). By feeding nonconscious processes proper stimuli, one can manipulate an individual's perception and ultimately their decisions Dijksterhuis, Smith, van Baaren and Wigboldus (2005); Kiesel, Wagener, Kunde, Hoffmann, Fallgatter and Stöcker (2006).

According to the world-renowned hacker and social engineer Kevin Mitnick, social engineering revolves around the adept use of influence and persuasion to deceive individuals, convincing them that the social engineer is someone else Mitnick and Simon (2003). Social engineering heavily targets the nonconscious mind, aiming to alter the victims' perception and ultimately manipulate their decisions without their awareness. As more attack vectors for social engineering are discovered, particularly in online environments Krombholz, Hobel, Huber and Weippl (2015), there is a growing recognition of the need to delve deeper into the psychological dimensions of security Enrici, Ancilli and Lioy (2010); Schneier (2015). This recognition underscores the necessity for further research in this domain, as current understanding remains superficial and fragmented across existing literature Montañez, Golob and Xu (2020).

Examining history's most significant social engineering attacks is crucial for comprehending their constituent

ORCID(s): 0009-0008-6490-6721 (I. Stylianou); 0000-0001-8155-1784 (P. Bountakas); 0000-0002-8480-6989 (A. Zarras); 0000-0001-6718-122X (C. Xenakis)

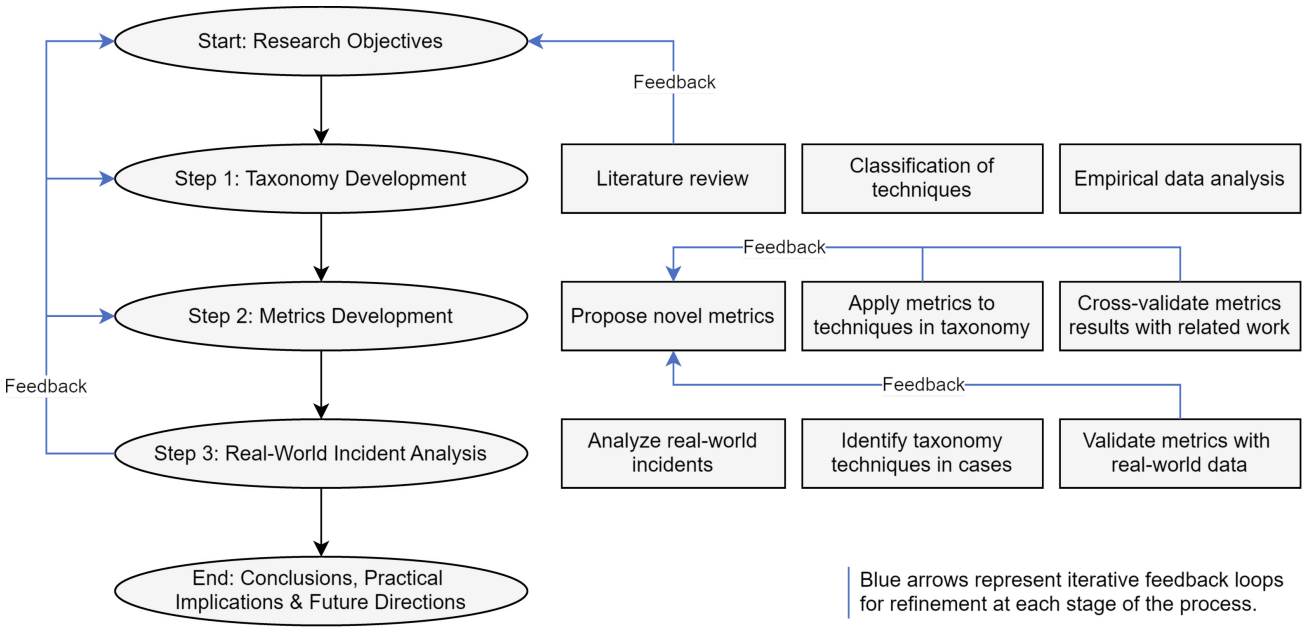

Figure 1: Flowchart of the Iterative Research Methodology

elements. Upon scrutinizing these prominent examples, it becomes evident that they all heavily leverage psychological tactics to achieve their objectives Enrici et al. (2010); Schneier (2015). To tackle this issue, this article offers a fresh perspective on online social engineering attacks by employing insights from psychology. The chosen approach involves a threefold methodology designed to address the research objectives comprehensively: (*i*) a thorough taxonomy of psychological techniques that are fragmented throughout the literature, (*ii*) novel metrics to quantitatively evaluate technique effectiveness, and (*iii*) a real-world incident case analysis. These components collectively investigate compliance-enhancing psychological techniques, evaluate their application in online social engineering attacks, and empirically compare their effectiveness for academic and practitioner needs. Figure 1 illustrates the iterative methodology employed in this research. Taxonomy development, metrics creation, and real-world validation work together through feedback loops to refine the framework continuously. This iterative approach mirrors continuous integration and continuous deployment (CI/CD) cycles, ensuring robust and adaptive results. To the best of our knowledge, no prior study has focused on investigating and applying contemporary psychological tactics in social engineering attacks, nor has any sought to compare the efficacy of established techniques. This interdisciplinary approach is poised to enhance our understanding of online social engineering attacks by amalgamating insights from both disciplines.

In summary, understanding the psychological techniques used in phishing is crucial, as these techniques form the core of phishing attacks by significantly enhancing the effectiveness of deception. This observation is reinforced by the real-world incidents analyzed in this study, which relied heavily on such psychological techniques. Currently, knowledge at the intersection of cybersecurity and psychology is superficial and fragmented across the literature. Existing research has not sufficiently examined how psychological principles can be applied within information security, nor has it assessed their impact on the success of cyberattacks. With the continuous proliferation of attack vectors in online environments Krombholz et al. (2015) and a prevailing focus on technical countermeasures, the current state of research fails to provide an adequate defense against phishing Enrici et al. (2010); Schneier (2015). Just as risk management principles suggest addressing the most severe risks first, it is necessary to identify and prioritize the most effective deceptive techniques. Since no suitable metrics previously existed, this study introduces new metrics to characterize and rank these techniques by their effectiveness under various circumstances discussed in Section 5, thereby allowing for an assessment of their relative severity.

In terms of practical implications and potential applications, this research offers cybersecurity professionals a comprehensive toolkit of psychological techniques, each evaluated for its effectiveness across different tasks. Newly emerging techniques can be rigorously measured and compared against established methods using the proposed framework. By evaluating and comparing emerging methods using this framework, practitioners can optimize training and improve detection solutions leveraging Natural Language Processing (NLP) and LLMs. This approach enables the incorporation of psychological techniques into State-of-the-art (SOTA) phishing detection, ultimately increasing accuracy.

Overall, this article makes the following contributions:

- A thorough, comprehensive taxonomy of psychological techniques correlated with online social engineering attacks is introduced.
- An analysis of real-world applications by identification and discussion of the implementation of psychological techniques in the most prominent real-life attacks.
- Novel metrics to evaluate the effectiveness of psychological techniques in a systematic and standardized way. Using these metrics, an effectiveness comparison of existing techniques across varying initial compliance circumstances has been performed. This approach not only enables a robust assessment of newly emerging techniques but also reveals critical insights into each technique's effectiveness under different compliance scenarios, as well as its comparative efficacy relative to others. The results were validated through comparison with previous literature Bullée, Montoya, Pieters, Junger and Hartel (2018).
- Future research directions have been identified and analyzed to drive much-needed research in the cross-disciplinary field of cybersecurity and psychology.

The remainder of this article is organized as follows. Section 2 provides a brief overview of related research and identifies its limitations. Section 3 delves into the analysis of psychological techniques. Section 4 explores the application of these techniques in specific online social engineering attacks. Their effectiveness is then compared in Section 5. Section 6 discusses the findings, research limitations and future research directions. Finally, Section 7 offers concluding remarks.

2. Related Work

Various related works, spanning from 1952 to the present, have been examined in this research, as summarized in Table 1. The literature review was conducted using a methodical approach to identify and compile all relevant works on compliance and conformity across multiple domains. Searches were performed primarily on Google Scholar and other academic databases (e.g. ACM Digital Library, ScienceDirect, IEEE Xplore, SpringerLink, arXiv), employing a broad range of keywords, including but not limited to compliance, conformity, persuasion, deception, social engineering, phishing, marketing psychology, behavioral psychology, and social psychology. No temporal limits were imposed. Specifically, we included only English-language works and prioritized peer-reviewed journal articles, conference proceedings, and academic books. Empirical studies were required to present original data on compliance/conformity phenomena; purely theoretical or opinion pieces without empirical support were excluded. The reviewed materials include journal articles, books, conference papers, and academic and non-academic sources. Inclusiveness served as the primary selection criterion, aiming to incorporate every documented technique and study related to compliance and conformity phenomena potentially applicable in online contexts. Cross-referencing and snowballing techniques ensured comprehensiveness, and references from key papers were examined. This final collection of literature embodies an interdisciplinary array of studies drawn from fields such as psychology, cybersecurity, and marketing. This section highlights the most relevant and significant works to identify existing gaps and emphasize the unique contributions of this research.

In Bullée et al. (2018), the authors analyze and dissect social engineering attacks found in literature works such as books or novels. The study categorizes techniques based on Cialdini's principles Cialdini (1984) and depicts the procedures used on each attack step in a tree form. However, a limitation of this work is that the analysis is not based on human participants and is limited to the specific techniques described in Cialdini's work.

Another study specializing in Internet scams Muscanell et al. (2014) is also based on Cialdini's principles Cialdini (1984). For each principle, the study analyses why individuals fall victim to Internet scams. Nevertheless, it does not incorporate any up-to-date techniques or present any data from psychological experiments that depict the effectiveness of different techniques.

In Krombholz et al. (2015), a taxonomy of known social engineering attacks is made based on the type of the attack, the channel through which it is carried, and the operator of the attack. The study also provides an overview of attack vectors and a discussion of real-world incidents. Even so, in this study, the psychological dimension is not considered, and no precautions to prevent or mitigate social engineering attacks are proposed.

Studies from the marketing field analyze how the consumer can be manipulated and how the unconscious influences their decision-making process respectively Dijksterhuis et al. (2005); Newell and Shanks (2014). Nonetheless, those studies are unrelated to social engineering and focus specifically on the consumer's psychology and the unconscious, respectively.

Another study analyzes how psychological dimensions have been taken into consideration in the recent literature on information security Enrici et al. (2010). The study concludes that *"it is hard to say that the psychological dimension of IT security may be considered nowadays a field of research"*. The study points out that the psychological dimension is usually omitted in information security and, therefore, highlights the importance of investigating the psychological dimension of security to avoid it being the weakest link that allows the chain of security to break. This study remarks on the lack of attention given to the psychological dimension without discussing any psychological techniques.

In Ferreira and Teles (2019), the authors study a sample of 194 phishing emails dated 2008-2017 to identify persuasion principles and present a method to define a tool for automated identification of principles of human persuasion. This research is based on NLP and does not analyze

Table 1
Overview of the Reviewed Literature

Type	Title	Year	Domain
Journal Article	Group forces in the modification and distortion of judgments	1952	Psychology
Journal Article	Opinions and social pressure	1955	Psychology
Journal Article	Studies of independence and conformity: I. A minority of one against a unanimous majority	1956	Psychology
Journal Article	Compliance, identification, and internalization three processes of attitude change	1958	Psychology
Journal Article	Compliance without pressure: The foot-in-the-door technique	1966	Psychology
Journal Article	Note on the drawing power of crowds of different size	1969	Psychology
Book	Social Psychology	1969	Psychology
Book	Social influence, conformity bias, and the study of active minorities	1972	Psychology
Miscellaneous	Obedience to authority: An experimental view	1974	Psychology
Journal Article	Reciprocal concessions procedure for inducing compliance: The door-in-the-face technique	1975	Psychology
Journal Article	Effects of Physical Attractiveness, Sex and Sex-Role on Trait Attributions	1977	Psychology
Journal Article	Low-ball procedure for producing compliance: Commitment then cost	1978	Psychology
Journal Article	Sex differences in influenceability	1978	Psychology
Journal Article	The mindlessness of ostensibly thoughtful action: The role of placebic information in interpersonal interaction	1978	Psychology
Book	The jigsaw classroom	1978	Psychology
Journal Article	Statistically combining independent studies: A meta-analysis of sex differences in conformity research	1979	Psychology
Miscellaneous	The Effects of Over Head Movements on Persuasion: Compatibility and Incompatibility of Responses	1980	Psychology
Journal Article	Sex differences in conformity: Surveillance by the group as a determinant of male nonconformity	1981	Psychology
Journal Article	Sex of researchers and sex-typed communications as determinants of sex differences in influenceability: a meta-analysis of social influence studies	1981	Psychology
Journal Article	The Perception of Androgyny and Physical Attractiveness	1983	Psychology
Book	Influence: The psychology of persuasion	1984	Psychology
Journal Article	Increasing compliance by improving the deal: The that's-not-all technique	1986	Psychology
Book	The robbers cave experiment: Intergroup conflict and cooperation.[Orig. pub. as Intergroup conflict and group relations]	1988	Psychology
Journal Article	The Attractiveness of Gender-Typed Traits at Different Relationship Levels: Androgynous Characteristics May Be Desirable after all	1994	Psychology
Journal Article	Culture and conformity: A meta-analysis of studies using Asch's (1952b, 1956) line judgment task	1996	Psychology
Journal Article	Influence of persuader gender versus gender of target on the selection of compliance-gaining strategies	1996	Psychology
Journal Article	The chameleon effect: The perception–behavior link and social interaction	1999	Psychology
Journal Article	Implicit cognition and the social unconscious	2002	Psychology
Book	The art of deception: Controlling the human element of security	2003	Cybersecurity
Journal Article	The chameleon effect as social glue: Evidence for the evolutionary significance of nonconscious mimicry	2003	Psychology
Journal Article	A multi-level defense against social engineering	2003	Cybersecurity
Journal Article	The Unconscious Consumer: Effects of Environment on Consumer Behavior	2005	Psychology
Journal Article	Unconscious manipulation of free choice in humans	2006	Psychology
Journal Article	Going along versus going alone: when fundamental motives facilitate strategic (non) conformity	2006	Psychology
Book	Influence: The psychology of persuasion	2007	Psychology
Journal Article	Social engineering: Exploiting the weakest links	2008	Cybersecurity
Miscellaneous	Obedience to authority	2009	Psychology
Journal Article	Persuasive systems design: Key issues, process model, and system features	2009	Psychology
Conference Paper	A psychological approach to information technology security	2010	Cybersecurity
Journal Article	Peer influence: neural mechanisms underlying in-group conformity	2013	Psychology
Journal Article	Weapons of Influence Misused: A Social Influence Analysis of Why People Fall Prey to Internet Scams	2014	Interdisciplinary
Journal Article	Unconscious influences on decision making: A critical review	2014	Psychology
Journal Article	Advanced social engineering attacks	2015	Cybersecurity
Book	Secrets & Lies: digital security in a networked world	2015	Cybersecurity
Conference Paper	Managing Social Engineering Attacks-Considering Human Factors and Security Investment	2015	Cybersecurity
Journal Article	Effects of Group Pressure Upon the Modification and Distortion of Judgments	2016	Psychology
Miscellaneous	Austrian Aeronautics Company Loses Over €42 Million to BEC Scam.	2016	Cybersecurity
Journal Article	On the anatomy of social engineering attacks-A literature-based dissection of successful attacks	2017	Interdisciplinary
Journal Article	The Influence of the Avatar on Online Perceptions of Anthropomorphism, Androgyny, Credibility, Homophily, and Attraction	2017	Psychology
Journal Article	Social engineering in cybersecurity: The evolution of a concept	2018	Cybersecurity
Journal Article	Hacking the human: The prevalence paradox in cybersecurity	2018	Interdisciplinary
Journal Article	Virtuous human hacking: The ethics of social engineering in penetration-testing	2019	Cybersecurity
Journal Article	The Influence of Age, Gender, and Cognitive Ability on the Susceptibility to Persuasive Strategies	2019	Psychology
Journal Article	Social engineering attacks: A survey	2019	Cybersecurity
Miscellaneous	Lithuanian Man Sentenced To 5 Years In Prison For Theft Of Over $120 Million In Fraudulent Business Email Compromise Scheme	2019	Cybersecurity
Journal Article	Persuasion: How phishing emails can influence users and bypass security measures	2019	Interdisciplinary
Journal Article	Group Conformity in Social Networks	2019	Psychology
Journal Article	Human cognition through the lens of social engineering cyberattacks	2020	Interdisciplinary
Miscellaneous	Analysis and Usage of Penetration Testing Tools	2021	Cybersecurity
Miscellaneous	7 of the biggest phishing scams of All time	2021	Cybersecurity
Journal Article	Phishing email strategies: Understanding cybercriminals' strategies of crafting phishing emails	2021	Cybersecurity
Journal Article	Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process	2021	Interdisciplinary
Book	Principles of Social Psychology-1st International H5P Edition	2022	Psychology
Miscellaneous	Stanley Milgram Shock Experiment: Summary, Results, & Ethics	2022	Psychology
Miscellaneous	5 of the most expensive phishing scams in history	2022	Cybersecurity
Miscellaneous	Office 365 phishing attack impersonates the US Department of Labor	2022	Cybersecurity
Miscellaneous	Obedience To Authority In Psychology	2023	Psychology
Miscellaneous	What is conformity?	2023	Psychology
Miscellaneous	The milgram shock experiment	2023	Psychology
Miscellaneous	Robbers Cave Experiment | Realistic Conflict Theory	2023	Psychology
Miscellaneous	5 worst whaling attacks: Whale phishing	2023	Cybersecurity
Miscellaneous	15 examples of real social engineering attacks	2023	Cybersecurity

the techniques psychologically or gauge their effectiveness. Similarly, in Stojnic, Vatsalan and Arachchilage (2021), the authors study phishing emails using NLP, topic modeling and clustering. There is a comparison between phishing and regular emails as well as topic words defined based on Gragg's psychological triggers Gragg (2003). This article does not study the psychological techniques, but rather the emails based on a subset of the techniques.

To summarize, existing work focuses on specific persuasion techniques, mostly from a psychological standpoint. Unfortunately, existing research lacks investigation into how those techniques can be applied in the information security field and fails to compare the techniques based on effectiveness. In order to address those limitations, this study includes a meta-analysis of psychological techniques based on empirical data, compares the effectiveness of the techniques using

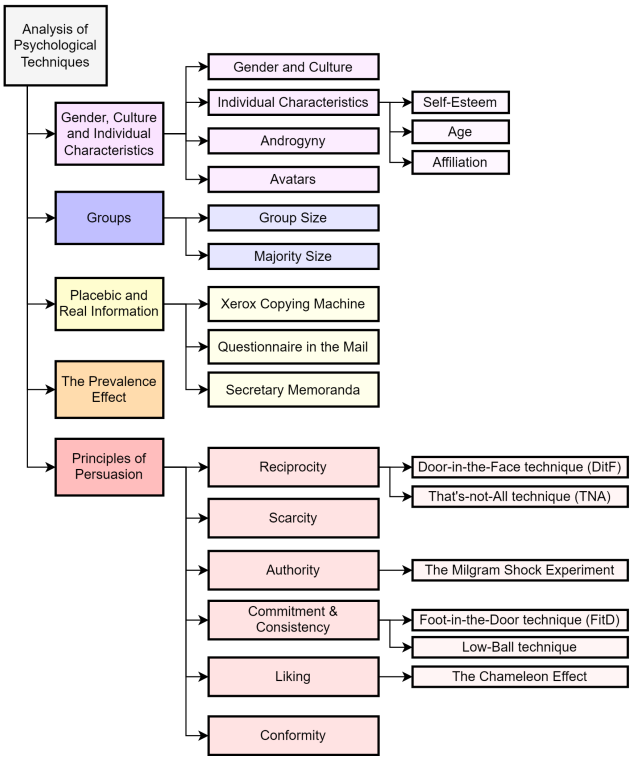

Figure 2: Analysis and Taxonomy of Psychological Techniques Tree of Contents

new metrics defined in this article, and examines how the techniques can be used in online social engineering attacks.

3. Taxonomy of Psychological Techniques

A systematic review and empirical analysis of several psychological techniques scattered throughout the literature provides a self-contained summary of each technique, its category, and empirical data from past experiments. The techniques included in this study represent a comprehensive collection of all compliance and conformity techniques identified across different sub-domains of psychology, including behavioral, social, and marketing psychology. Apart from the psychological domains that were deemed pertinent to social engineering, no additional selective criteria were applied, ensuring the taxonomy captures the full range of documented approaches. The results of the experiments have been formatted into tables and figures that are easy to comprehend, providing a dense and compact visualization of each technique's empirical outcomes and effectiveness. This approach facilitates a deeper investigation into how these techniques can be deployed in social engineering attacks (Section 4) and supports their subsequent comparison (Section 5). The taxonomy is depicted in Figure 2 and further elaborated in this section.

3.1. Gender, Culture, and Individual Characteristics

This section examines the influences of gender, culture, and individual characteristics on conformity and persuasion. We explore how different genders react within different contexts and analyze individual traits such as self-esteem, age, and affiliation, to understand their impact on persuasive outcomes. This analysis aims to highlight the complex interplay between personal and societal factors that shape behavioral responses and influence techniques in human interactions.

3.1.1. Gender and Culture

The role of gender in conformity has been investigated in several studies Cooper (1979); Eagly (1978); Eagly, Wood and Fishbaugh (1981); Abroshan, Devos, Poels and Laermans (2021). There is a difference regarding the conformity of men and women, where based on previous research Bond and Smith (1996); Cooper (1979); Abroshan et al. (2021), women are more likely to conform than men, however the scenario at hand is an important factor. More specifically, some research has found that women are more likely to conform to group norms and expectations than men, especially when it comes to matters of social etiquette and appearance, while men may be more likely to conform to group norms and expectations in situations where there is a clear hierarchy, or a need to assert dominance Jhangiani and Tarry (2022). However, the cultural setting of the surveys has been noted to be significantly related to conformity Bond and Smith (1996). Notably, conformity was greater in more collectivist than in individualist countries. Factors such as socialization, expectations, and power dynamics play an essential role. It is interesting to note that men are less likely to conform when they are observed Eagly (1978); Eagly et al. (1981), possibly to be compatible with their societal role as independent and confident, or to try to influence the rest of the group Eagly et al. (1981). Later studies have shown that men resist conformity in order to demonstrate their quality as mates when they are being persuaded after having romantic thoughts and sexual attraction Griskevicius, Goldstein, Mortensen, Cialdini and Kenrick (2006).

Aside from that, there has been evidence to show that different techniques are more effective when used against different genders Abdullahi, Oyibo, Orji and Kawu (2019) and that the combination of sexes of the persuader and persuadee is also important Hertzog and Scudder (1996). Abdullahi et al. (2019) conclude that males are more likely to be susceptible to social learning[1], while females are more likely to be susceptible to reward[2] and trustworthiness[3]. All definitions for social learning, reward and trustworthiness are based on Oinas-Kukkonen and Harjumaa (2009). According to Hertzog and Scudder's research Hertzog and Scudder (1996), men use impersonal commitments and expertise to persuade women while they prefer punishing and expertise in some cases to have other men conform. On the other hand, women tend to use mainly impersonal and sometimes personal commitments when persuading men, while

[1] A persuasive strategy that allows a user to observer the behaviors of others in the hope that they will be influenced in one way or the other to behave in a similar way.

[2] Offering incentives to users for performing a target behavior.

[3] The strategy to motivate users to adopt and/or use a system by enhancing their perceived trust in the system and the services it offers.

they shift to a combination of mostly expertise accompanied by personal commitments and rewards to persuade other women. To the best of our knowledge, based on the literature reviewed to date there have been no further studies that expand upon or update the findings of gender combinations in persuasion.

Hertzog and Scudder's study Hertzog and Scudder (1996) included 120 students (46 males and 76 females) who were asked to write in detail about the most recent instance in which they had to persuade someone else to comply. The experiment showed that persuader-target gender pairings affect compliance rates. Specific suitability metrics for different approaches for different gender combinations can be found in the study.

3.1.2. Individual characteristics

The characteristics of the person being persuaded affect the success rate of the persuasion mechanism and in turn the efficacy of the social engineering attacks. The following individual characteristics matter when persuading someone Jhangiani and Tarry (2022):

Self-esteem: Lower self-esteem creates a higher need to belong, which in turn increases the need for approval, thus increasing conformity.

Age: People below 40 are more likely to be influenced.

Affiliation: People affiliated with the group creating conformity are likelier to conform.

It is important to note that the effect of a person's individual characteristics on conformity is less relevant than that of social variables. Increasing the unanimity or the number of the group has more significant effects on the compliance rate.

3.1.3. Androgyny

Androgynous people are often perceived more favorably than traditionally sex-typed or sex-reversed roles according to several studies Green and Kenrick (1994); Jackson (1983); Major and Deaux (1977); Nowak and Rauh (2017). Androgyny seems to have a greater positive impact for women, who were evaluated higher in all dimensions, than it does for androgynous men, who were rated less assertive and masculine Major and Deaux (1977), although the findings of Green and Kenrick Green and Kenrick (1994) show similar favorability for androgynous male and female targets compared to their traditionally gender-typed [4] roles. Green and Kenrick's experiment included four gender-type combinations (i.e., androgynous, masculine, feminine, and undifferentiated) and two variables (i.e., instrumentality—consisting of traits such as being independent, active, competitive, decisive, never giving up, superior, standing up well under pressure, self-confident and expressiveness—consisting of traits such as being emotional, devoted to others, gentle, kind, aware of feelings of others, understanding, helpful, warm). The different combinations can be found in Table 2

Table 2
Level of instrumentality and expressiveness for different type of people (▲ symbol is used for high and ▼ symbol for low)

Profile	Instrumentality	Expressiveness
Androgynous	▲	▲
Masculine	▲	▼
Feminine	▼	▲
Undifferentiated	▼	▼

Table 3
Results of the Androgyny Experiment

	Instrumentality		Expressiveness	
	Low	***High***	***Low***	***High***
Male	4.55	6.68	3.61	7.25
Female	2.6	6.81	3.01	7.16

Participants, consisting of 135 females and 86 males, completed a Personal Attributes Questionnaire (PAQ) for each of the four gender-type combinations. Subsequently, they were instructed to assess the attractiveness of the depicted individuals using a scale ranging from 1 to 9. This process was repeated, with participants providing information regarding the individuals' instrumentality or expressiveness traits while withholding any contradictory details from the questionnaire.

The findings revealed a preference for targets exhibiting high instrumentality and high expressiveness. Female participants ranked males with high expressiveness and low instrumentality as their second choice, contrary to the expected preference for gender-typed males with high instrumentality and low expressiveness. Figure 3 provides a visual summary of the experiment's results included in Table 3, with the y-axis denoting participants' ratings of the desirability of individuals across different gender types.

3.1.4. Avatars

People often represent themselves online in today's society. Anthropomorphic avatars were viewed as more attractive and credible Nowak and Rauh (2017). Feminine avatars were reported to be more attractive compared to masculine avatars. With many social engineering attacks occurring online, such as phishing attacks performed via social media or messaging platforms, the avatar of choice of the attacker could play a role in the performance of the attack.

3.2. Groups

People's interaction in group settings has been observed to heavily affect their reasoning. People tend to conform when imposed with the pressure of a group's opinion Asch (2016, 1952, 1956). This has also been observed in online settings, as seen in the research of Morrison and Naumov

[4] Behaviors, traits, and social roles commonly associated with a specific gender in society, often perpetuated through cultural norms and socialization processes.

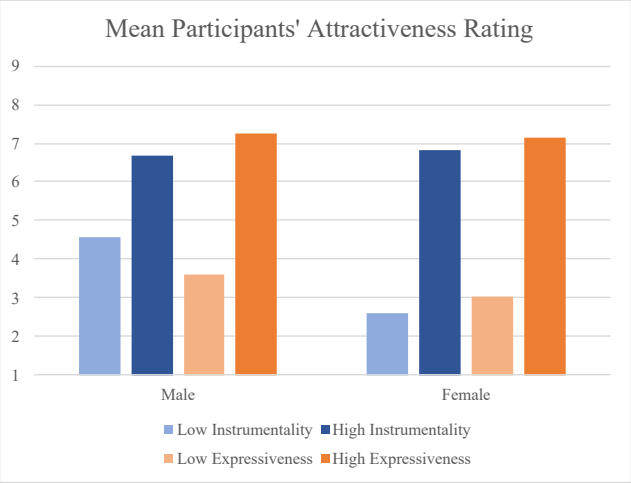

Figure 3: Androgyny as a Determinant in Influenceability Green and Kenrick (1994)

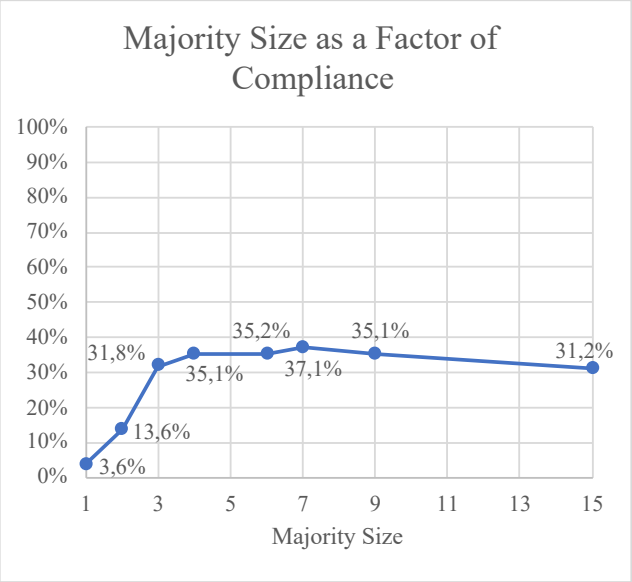

Figure 4: Group size as a Determinant in Influenceability Asch (1955)

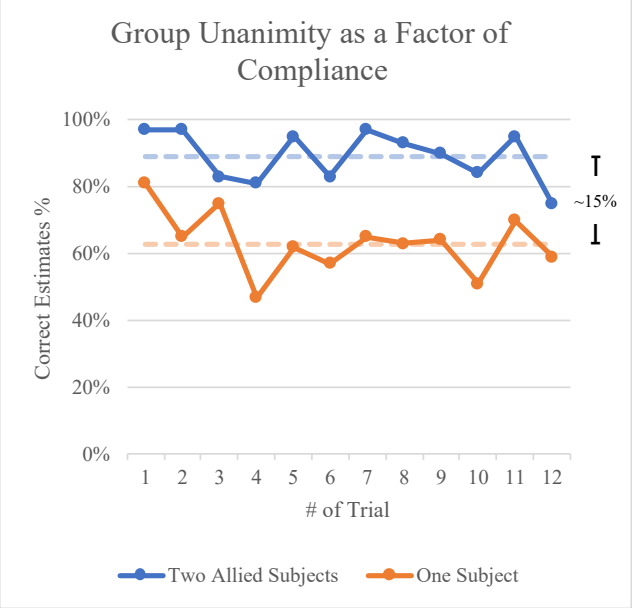

Figure 5: Group unanimity as a Determinant in Influenceability Asch (1955)

(2019). Further studies have used functional magnetic resonance imaging (fMRI) technology to explore the underlying mechanisms that cause this behavior, which confirmed this observation Stallen, Smidts and Sanfey (2013). Solomon Asch's experiments focused on just that. The participant was placed in a group and was asked to match the length of each given line to any of three possible answers. There were 18 trials, 12 of which were critical (where the group gave a unanimous erroneous answer). Everyone else in the group gave a contradicting—while obviously incorrect—answer. Asch's study included 50 male participants in the Critical/Experimental group and 37 male participants in the control group. The results for the Experimental Group were the following:

- Never conformed: 26%
- Conformed on at least one trial: 74%
- Always conformed: 5%
- Average conformity: 32% of the critical trials (192 errors on 600 trials)
- All errors of the critical group were towards the estimation of the majority
- Control group error rate: 1 person made 1 error; 1 person made 2 errors. There were a total of 3 errors in $37 \cdot 12 = 564$ trials (0.54% error rate)

Further experiments Asch (1956) conducted by Asch, such as related experiments on drawing the attention of passersby Milgram, Bickman and Berkowitz (1969), show that the optimal group size (without including the target of the experiment) is three to five individuals as shown in Figure 4. The group's unanimity is highly significant; the presence of an "ally" in the group (who always answered correctly) drastically drops the levels of conformity as illustrated in Figure 5.

3.3. Placebic and Real Information

Three different experiments were conducted to test the mindfulness and consciousness of the participants' social behavior by receiving different communications with the following properties Langer, Blank and Chanowitz (1978):

- Semantically sensible or not
- Structurally consistent with previous experience or not
- Requesting an effortful response or not

Table 4
Results of the Xerox Copying Machine Experiment

	Request	Placebic	Real
Small (5 pages)	60% (9/15)	93% (14/15)	94% (15/16)
Large (20 pages)	24% (6/15)	24% (6/15)	42% (10/24)

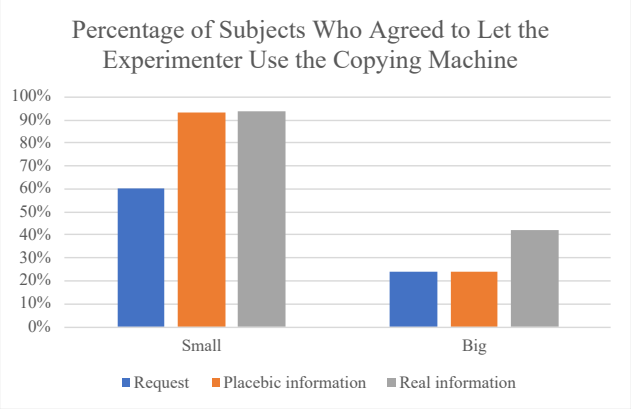

Figure 6: Xerox Copying Machine Compliance Rate

In the following sections, we analyze these experiments to gain insights regarding placebic information, congruity, and requested effort in persuasion.

3.3.1. Xerox Copying Machine

For the first experiment regarding placebic information, the experimenter sat at a table in the library where they had a clear view of the copier. When a participant used the copier and placed their material on the machine, the experimenter approached them right before they deposited the money to begin copying. The participant asked the experimenter to use the machine first to copy 5 or 20 pages. If the experimenter had fewer pages to copy than the participant, this constitutes a small favor. Otherwise, the favor is considered to be large.

The experimenter used three different phrases to perform the request:

- **Request:** "Excuse me, I have (5/20) pages. May I use the xerox machine?"
- **Placebic information:** "Excuse me, I have (5/20) pages. May I use the xerox machine, because I have to make copies?"
- **Real information:** "Excuse me, I have (5/20) pages. May I use the xerox machine, because I'm in a rush?"

The results of the experiment can be summarized in Table 4, as well as on Figure 6:

The experiment shows that, for small requests, people accept placebic information as an equally valid reason as real information and are more likely to comply. When the favor becomes larger, the offender needs to incorporate real information to urge the victim to comply. The offender can manipulate their victim into complying using either placebic information for a small request or relevant information in favor of a greater scale.

Table 5
Results of the Questionnaire Experiment (Congruity)

	High Status	Random Status
Congruent	55% (11/20)	20% (4/20)
Incongruent	32% (6/19))	37% (7/19)

Table 6
Results of the Questionnaire Experiment (All Combinations)

	High Status		Random Status	
	Personal	***Impersonal***	***Personal***	***Impersonal***
Demand	33% (3/9)	40% (4/10)	44% (4/9)	20% (2/10)
Request	70% (7/10)	30% (3/10)	20% (2/10)	30% (3/10)

3.3.2. Questionnaire in the Mail

For the second study on placebic information, eighty (80) randomly selected participants were mailed a questionnaire containing five unimportant questions. The participants were of different *status* Langer et al. (1978):

- 40 of the participants were from the Manhattan telephone directory.
- 40 of the participants were from the "Physicians" section of the Manhattan Yellow pages.

The *conditions* of every letter varied between congruent/incongruent, request/demand, personal/impersonal, creating $2 \times 2 = 4$ combinations:

- **Request:** "I would appreciate it if you would fill out the attached questionnaire and return it in the enclosed envelope to me by September 10."
- **Demand:** "The attached questionnaire is to be filled out and returned by September 10."
- **Personal:** The letter was signed "Thank you for your help, George L. Lewis."
- **Impersonal:** The letter was without any signature.

The letters are characterized as congruent/incongruent based on the congruity of the request/demand and personal/impersonal variables:

- **Congruent:** Either a personal request or an impersonal demand
- **Incongruent:** Either a personal demand or an impersonal request

The results of the experiment can be summarized in Tables 5 and 6, as well as on Figures 7 and 8:

Personal style seems to have had a higher average success rate for high-status and random-status participants and

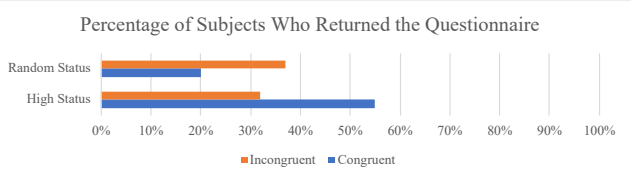

Figure 7: Questionnaire Compliance Rate with respect to Congruity

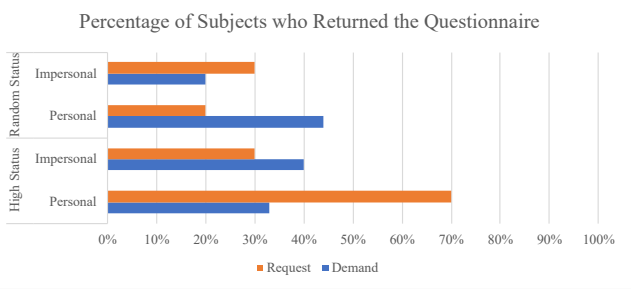

Figure 8: Questionnaire Compliance Rate 2×2 matrix

would be the go-to method for an offender. Personal requests had an incredible success rate against high-status targets, while personal demands had the same effect for random-status targets. High-status targets are more volatile to congruent conditions. Random status targets are unaffected by conditions.

3.3.3. Secretary Memoranda

For the third experiment on placebic information, eighty-three (83) memoranda were first collected from waste baskets of 20 secretaries at the Graduate Center on the premises of the City University of New York Langer et al. (1978). The majority (68%) of the memoranda had an impersonal request structure, while the remaining 32% were evenly distributed between the remaining categories. Thus, the congruent form for this experiment was made up of solely impersonal requests. The other three possibilities, impersonal demands, personal requests, and personal demands, were viewed as incongruent.

For this experiment, 40 secretaries at the Graduate Center were sent a memorandum through office mail. The email forms were requests/demands in personal/impersonal form:

- **Request:** "I would appreciate it if you would return this paper immediately to Room 238 through interoffice mail."
- **Demand:** "This paper is to be returned immediately to Room 238 through interoffice mail."
- **Personal:** "Sincerely, John Lewis".
- **Impersonal:** Simply had a number (R374021-A) appended after the message.

The experiment's goal is similar to that of second experiment: to examine how different conditions affect the

Table 7
Results of the Secretary Memo Experiment

	Personal	Impersonal
Demand	60% (6/10)	50% (5/10)
Request	70% (7/10)	90% (9/10)

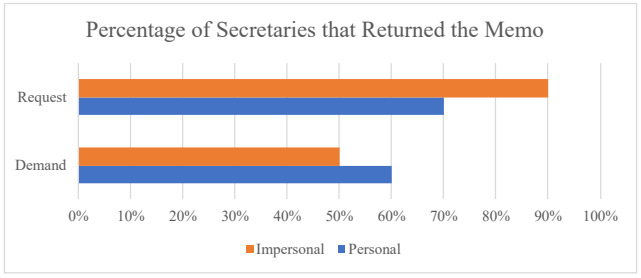

Figure 9: Secretary Compliance Rate with respect to Conditions

percentage of participants who return the memo. The results can be summarized in Table 7 and Figure 9.

The percentage of participants that returned the memo in congruent conditions (impersonal request: 90%) compared to the participants in congruent conditions (mean of other conditions: 60%) were shown to be significantly different using 0 and 1 scores ($t(38) = 1.78, p < .05$).

People tend to comply more when faced with a request rather than a demand. People are much more likely to comply with a request congruent with their actions' regular conditions. An offender can maximize the effectiveness of a social engineering attack by studying the victim's conditions to plan the attack accordingly, using the proper request style.

3.4. The Prevalence Effect

The prevalence effect is the psychological phenomenon that rare signals are harder to detect, even when taking into account their significantly low probability of occurring. In fact, as the signal probability diminishes, the accuracy with which one can recognize the signal decays logarithmically Sawyer and Hancock (2018).

An experiment to show how the prevalence effect can be applied to social engineering, particularly phishing, was executed. The participants received emails for a specific period, asking them to either download a PDF file or upload an existing one. After reading an email in their inbox, the participants of the study could perform one of the following three actions:

- Download attachments.
- Reply and upload their own attachments.
- Report said message as possibly malicious.

The nature of the emails was one of the following:

- **Legitimate:** Sent from email addresses under a specific domain ending in ".com".

- **Malware:** The file attached would be an executable (.exe) file instead of a .pdf file.
- **Phishing:** The email would have a sender address with the ".tv" top-level domain instead.

The participants were divided in three (3) different groups, with the signal probability being 1%, 5%, 20% respectively. The signal probability was not known to them, and the emails were evenly distributed between upload and download tasks. The measurements made to estimate the participants' performance were in regards to their rate of reported malicious emails per total amount of malicious emails (accuracy), as well as the average time spent per email (response time). The results of the experiment are presented visually in the research of Sawyer and Hancock (2018), comparing the performance indicators—response accuracy and response time—for every group with a different signal probability (SP), as well as the response accuracy with respect to different SP.

The results show that the participants of the low signal probability group (1% SP) detected malicious emails at a significantly lower rate despite allocating more time to decide for each email. Furthermore, the logarithmic fit for the data retrieved from the experiment is better than the linear fit, suggesting that, as seen in past research regarding the prevalence effect, the pattern found is one of logarithmic decay of accuracy as signal probability (SP) approaches zero Sawyer and Hancock (2018).

The prevalence paradox is that having a well-configured email filtering system reduces the signal probability of a malicious email being sent to an employee, and therefore, the employee has an ever-increasing chance to detect the remaining malicious emails the better the filtering system is Sawyer and Hancock (2018).

3.5. Principles of Persuasion

The principles of persuasion are properties of the offender that can influence the target's behavior, increasing the odds of compliance to the offender's favor Bullée et al. (2018). The principles constitute the following Cialdini (2007): (*i*) reciprocity, (*ii*) scarcity, (*iii*) authority, (*iv*) commitment & consistency, (*v*) liking, and (*vi*) conformity (social proof/unity).

3.5.1. Reciprocity

The technique of reciprocity involves the offender giving something in return. This puts the offender in an advantageous position as the target feels indebted to the requester for their gesture, even though the actual gift might be insignificant. This allows the offender to implement quid pro quo attacks. The Latin expression "quid pro quo" translates directly to "something for something" and implies an exchange of services or goods. The victim is made to believe that the exchange is fair, but the benefit for the attacker is significantly greater Stylianou (2021). Two main techniques utilize this technique, the Door-in-the-face technique and the That's-not-all technique.

Table 8
Results of the Door-in-the-face experiment 1

	Smaller request only	Exposure	Rejection-moderation (DitF)
Compliance %	16.7% (4/24)	25% (6/24)	50% (12/24)

Door-in-the-Face technique (DitF). A typical technique under this category is the DitF technique. When performing this technique, the persuader initially makes an unrealistic request that the respondent turns down and then makes a more reasonable request the respondent will feel compelled to accept, as they feel they owe the persuader. Cialdini performed three experiments Cialdini, Vincent, Lewis, Catalan, Wheeler and Darby (1975) to test the effectiveness of this technique.

In the study's first experiment, 72 participants of both sexes strolling alone through university walkways in the daytime were selected. Either of the following requests were made by the experimenter:

- **Large request:** If they would like to be considered for working as voluntary, nonpaid counselors at the County Juvenile Detention Center (2 hours/week for at least 2 years.
- **Small request:** If they would like to be considered for working as voluntary, nonpaid chaperones for a group of children from the County Juvenile Detention Center on a trip to the zoo (2 hours of one afternoon or evening.

Three different conditions were studied:

- **Smaller Request Only Control Condition:** Participants were only asked to perform the small request.
- **Exposure Control Condition:** Participants heard both requests and were then requested to perform either.
- **Rejection-moderation Experimental Condition:** Participants heard the extreme request first, and after refusing, the experimenter elaborated on the smaller request after saying "Well, we also have another program you might be interested in then".

Considering no participant agreed to the larger favor, the experiment's results regarding the small favor can be summarized in Table 8 and Figure 10.

A second experiment was conducted to test whether the participants showed greater compliance due to perceiving asking a smaller favor as a concession by the requester. If this were the case, the participants would not be more compliant if a different person made the smaller second request. For this experiment, 58 males were selected using the same procedure as in the first experiment. Either of the following requests were made by the experimenter:

- **Large request:** If they would like to be considered for working as voluntary, nonpaid counselors at the

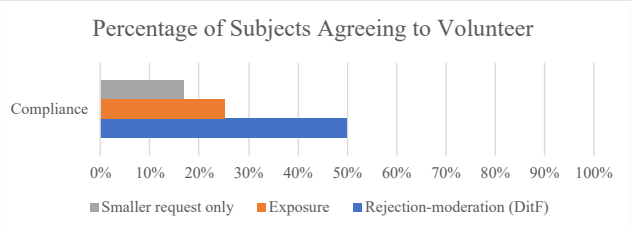

Figure 10: Compliance using Door-in-the-Face Technique (Experiment 1)

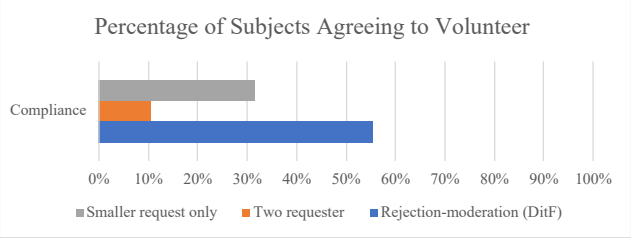

Figure 11: Compliance using Door-in-the-Face Technique (Experiment 2)

Table 9
Results of the Door-in-the-face experiment 2

	Smaller request only	Two requester	Rejection-moderation (DitF)
Compliance %	31.5% (6/19)	10.5% (2/19)	55.5% (11/20)

County Juvenile Detention Center (2 hours/week for at least 2 years.

- **Small request:** If they would like to be considered for working as voluntary, nonpaid chaperones for a group of "low-income children" on a trip to the zoo (2 hours of one afternoon or evening).

The following conditions were studied:

- **Smaller Request Only Control Condition:** Participants heard the small request only.
- **Two-requester Control Condition:** Participants heard the extreme request first, and after refusing, the experimenter left, while a different experimenter made the small request, as if he overheard the discussion.
- **Rejection-moderation Experimental Condition:** Participants heard the extreme request first, and after refusing, the experimenter elaborated on the smaller request.

The experiment results summarized in Table 9 and Figure 11 show that the concept of concession is important. When the same experimenter conceded, the participants were more inclined to reciprocate the concession.

A third experiment was performed to test whether the participants showed greater compliance after being pressured with a second request. For this experiment, 72 participants of both sexes were included, and the following conditions were studied:

Table 10
Results of the Door-in-the-face experiment 3

	Smaller request only	Equivalent request	Rejection-moderation (DitF)
Compliance %	33.3% (8/24)	33.3% (8/24)	54.1% (13/24)

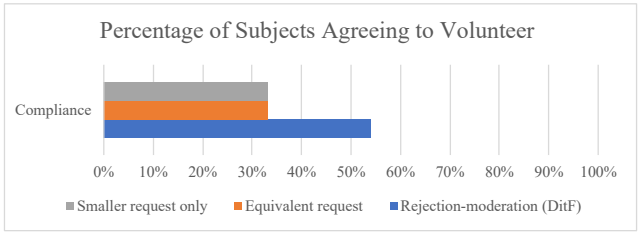

Figure 12: Compliance using Door-in-the-Face Technique (Experiment 3)

- **Smaller Request only Control Condition:** Identical to the same condition of Experiment 1.
- **Equivalent Request Control Condition:** Participants heard an initial request for being chaperones for juvenile delinquents during their 2 hour trip to the city museum. After responding, the second request was chaperoning for juvenile delinquents during a 2 hour trip to the zoo.
- **Rejection-moderation Experimental Condition:** Identical to the same condition of Experiment 1.

The experiment results summarized in Table 10 and Figure 12 show that it was not the pressure of a second request that increased compliance.

That's-not-All technique (TNA). Another technique initially observed in the context of marketing and sales is the "that's not all technique". When performing this technique, the persuader shows a deal to the respondent. Before the respondent has a chance to reply, the persuader adjusts the offer usually by lowering the price or adding an extra product. The respondent feels inclined to accept the offer, perceiving the persuader's TNA statement as generosity that they need to reciprocate. This technique was tested in several experiments by Burger (1986), four of which are pertinent to this research.

The first experiment Burger (1986) investigates the effect of adding an extra product. The participants of the experiment included 60 adults and teenagers that approached either of three booths set up at different locations. All booths announced the psychology club's bake sale, with cupcakes on display without a labeled price. People that approached the two experimenters standing in the booth and inquired about the price were given either of the following responses:

- **TNA Experimental Condition (product addition):** The participants were told that the cupcakes were 75 cents each. The second experimenter tapped the first on the shoulder and the first continued to say "wait a second". The experimenters discussed for a couple of

Table 11
Results of the That's-not-All experiment 1 (Product Addition)

	Control Condition	Experimental Condition (TNA - Product Addition)
Compliance %	40% (12/30)	73% (22/30)

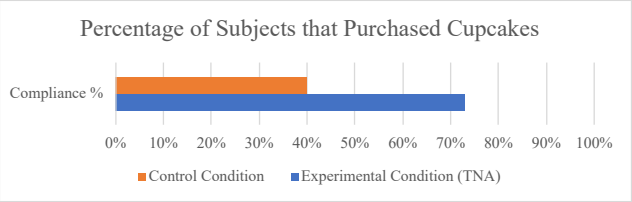

Figure 13: Compliance using That's-not-All Technique - product addition (Experiment 1)

Table 12
Results of the That's-not-All experiment 2 (Price Reduction)

	Control Condition	Experimental Condition (TNA - Price Reduction)
Compliance %	44% (12/27)	73% (19/26)

seconds and then the first experimenter added that the price includes two cookies, which were displayed only then.

- **Control Condition:** The participants were shown the cookies and were told about the complete package for 75 cents as soon as they inquired.

The results of the experiment shown in Table 11 and Figure 13 show a statistically significant correlation between usage of the TNA technique (product addition) and participant compliance, $x^2(1, N = 60) = 6.79, p < .01$. Similarly to the DitF technique, the participants were more inclined to make concessions when the experimenter made a concession to them.

The second experiment Burger (1986) examines the effect of reducing the price. The participants were 53 of the same demographic and the conditions were modified accordingly:

- **TNA Experimental Condition (price reduction):** The participants were told that the cupcakes were a dollar each. The second experimenter tapped the first on the shoulder and the first continued to say "wait a second". The experimenters discussed for a couple of seconds and then the first experimenter added that they will be selling them for 75 cents instead because they will be closing soon.
- **Control Condition:** The participants were told that the cupcakes were sold for 75 cents each.

The results of the experiment shown in Table 12 and Figure 14 show a statistically significant correlation between usage of the TNA technique (price reduction) and participant compliance, $x^2(1, N = 60) = 4.47, p < .05$.

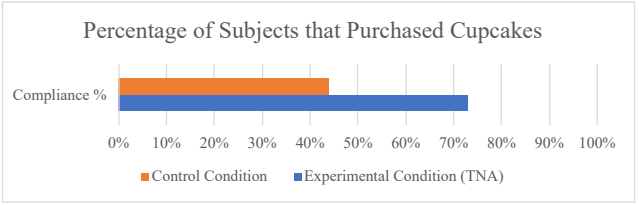

Figure 14: Compliance using That's-not-All Technique - price reduction (Experiment 2)

Table 13
Results of the That's-not-All experiment 3 (Negotiation)

	Control Condition	TNA - Negotiation	TNA - No-negotiation
Compliance %	50% (10/20)	85% (17/20)	70% (14/20)

The third experiment Burger (1986) examines the importance of the concession feeling personal or something the seller is forced to do. The participants were 60 of the same demographic and the conditions were modified accordingly:

- **TNA Experimental Condition (negotiation):** The participants were told that the cupcakes were a dollar each. The second experimenter tapped the first on the shoulder and the first continued to say "wait a second". The experimenters discussed for a couple of seconds and then the first experimenter added that he wanted to leave soon so they would be willing to sell them for 75 cents each instead.
- **TNA Experimental Condition (no-negotiation):** The participants were told that the cupcakes were a dollar each. The second experimenter tapped the first on the shoulder and the first continued to say "wait a second". The experimenters discussed for a couple of seconds where the second experimenter said the cupcakes really sell for 75 cents loud enough for the participant to hear. The first experimenter went on to justify their mistake by mentioning they started selling that day and that these cupcakes were really 75 cents each.
- **Control Condition:** The participants were told that the cupcakes costed 75 cents each.

The results of the experiment shown in Table 13 and Figure 15 show a statistically significant correlation between usage of the TNA technique (negotiation) and participant compliance, $x^2(1, N = 60) = 5.58, p < .02$. The usage of the TNA technique (no-negotiation) did not have significant effects.

The fourth experiment Burger (1986) is a modified version of the third experiment, implementing a door-to-door approach, where the experimenters attempt to sell candles for a school's expenses to 105 adults of a middle-class neighborhood. The conditions were modified as follows:

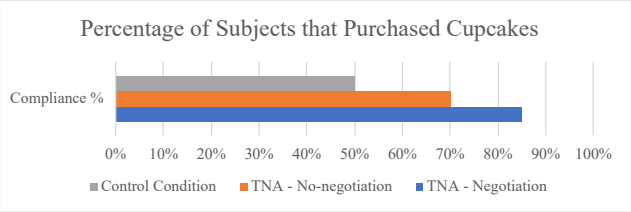

Figure 15: Compliance using That's-not-All Technique - negotiation (Experiment 3)

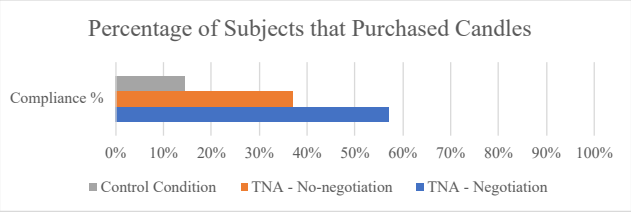

Figure 16: Compliance using That's-not-All Technique - negotiation variation (Experiment 4)

Table 14
Results of the That's-not-All experiment 4 (Negotiation variation)

	Control Condition	TNA - Negotiation	TNA - No-negotiation
Compliance %	14.3% (5/35)	57.1% (20/35)	37.1% (13/35)

- **TNA Experimental Condition (negotiation):** The participants were told that the candles were 3 dollars. The second experimenter tapped the first on the shoulder and the first continued to say "excuse me". The experimenters discussed for a couple of seconds and then the second experimenter said they decided to sell them for 2 dollars loud enough for the participant to hear. The first experimenter went on to apologize for their mistake and verify that the price was 2 dollars in order to try to sell more candles at a lower price.
- **TNA Experimental Condition (no-negotiation):** The participants were told that the candles were 3 dollars. The second experimenter interrupted the first and said that they sold all of the 3 dollar candles and these were 2 dollar candles. The first experimenter went on to apologize for their mistake and verify that the price was 2 dollars.
- **Control Condition:** The participants were told that the candles were 2 dollars.

The results of the experiment shown in Table 14 and Figure 16 showed a statistically significant correlation between usage of the TNA technique (negotiation) and participant compliance, $x^2(1, N = 70) = 14.00, p < .001$. The usage of the TNA technique (no-negotiation) also had significant correlation, $x^2(1, N = 70) = 4.79, p < .05$. The difference between the TNA conditions was only marginally significant, $x^2(1, N = 70) = 2.81, p < .10$. These results along with the previous experiment show that reciprocity enhances the effectiveness of the TNA technique, but the technique is also effective without it.

3.5.2. Scarcity

The scarcity technique is implemented when the offender persuades the individual that the product or service offered has limited availability Bullée et al. (2018). The victim tends to overestimate the value of said service or product, and has an increased probability to comply with the offender's plan. As shown by the "Robbers Cave Experiment", people tend to compete for limited resources to the point they become hostile to each other Sherif (1988); Saul (2023a).

3.5.3. Authority

The likelihood of a victim complying with a request is higher, when the request is made by an authoritative figure Saul (2023a). Stanley Milgram, a psychologist at Yale University, conducted an experiment to evaluate how far people would go when influenced into a decision by an authoritative figure. The experiment is known as the "Milgram Shock Experiment". The trigger for Milgram to perform the experiment was the fact that many of the defendants accused during the World War II, Nuremberg War Criminal trials claimed that they were just obedient to their superiors, following their orders.

Preparation. The experiment was advertised as a learning, controlled[5] experiment and took place in Yale university's Interaction Laboratory Milgram (1974). Milgram recruited 40 male volunteers, with ages of 20-50, and varying jobs from unskilled to professionals, who lived in New Haven. The volunteers were paid $4.50 for participating.

Execution. Once the experiment started, each participant was introduced to one of Milgram's associates, who was disguised as a fellow participant. The two participants drew straws to decide which would be the "learner" and which would be the "teacher", but Milgram's associate would always get the role of the learner and the actual participant the role of the teacher. The "teacher" participant was given a sample 45 V shock. The "learner" was strapped to a chair with electrodes in one room and given a list with pairs of words to memorize. After the "learner" learned the words, the "teacher" read a word and asked the "learner" to pick the word paired with it from four possible choices. The "teacher" participant sat in an adjacent room, in front of a replica shock generator.

The "experimenter" told the "teacher" to administer a shock for each mistake, starting from 15 V and incrementing the voltage by 15 volts each time. In reality, though, there were no shocks. The shock generator had 30 switches from 15 to 450 Volts with 15 V increments. Every group of switches is labeled as in Fig 17.

[5] An experiment where all factors are constant except the independent variable, in order to scientifically test a hypothesis.

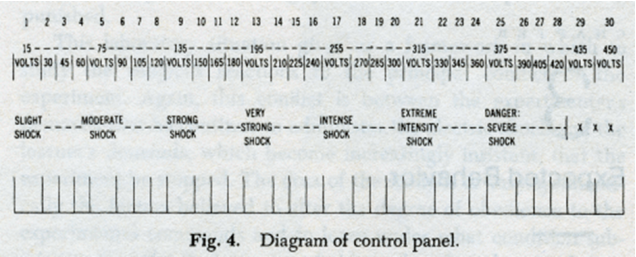

Fig. 4. Diagram of control panel.

Figure 17: The device's control panel Milgram (1974)

The "learner" purposely answered incorrectly most of the time, and the "teacher" gave them an electric shock. When the "teacher" refused to comply, the experiment cycled through the following different phrases Milgram (1974):

- "Please continue." or "Please go on."
- "The experiment requires that you continue."
- "It is absolutely essential that you continue."
- "You have no other choice, you must go on."

In case the participant asked if the "learner" could suffer permanent damage the experiment used the special phrase Milgram (1974): "Although the shocks may be painful, there is no permanent tissue damage, so please go on." The victim had predetermined responses:

- No discomfort until 75 V.
- A grunt for 75-105 V.
- Victim shouts to the experimenter that the shocks are painful at 120 V.
- Painful groans at 135 V.
- Victim cries out to be let out of the room and quit the experiment from 150 V onward.
- Victim cries out that they could not stand the pain at 180 V.
- Agonizing scream by 270 V.
- Shouts in desperation that they will no longer provide answers at 300 V.
- After 330 V they are neither heard from nor have any answers appear on the signal-box.

Prediction and Outcome. Prior to the study, Milgram asked a group of experts (psychiatrists, graduate students, behavioral-science faculty, college sophomores, and middle-class adults) to estimate how many individuals out of a hypothetical group of 100 Americans (diverse in age and occupation) acting as "teachers" would administer at least a 300 V shock and how many would go on to the full 450 V. Their average estimate was that 3.73% would reach 300 V, and only 0.125% would reach the maximum 450 V. In contrast, 100% of the participants actually administered at least 300 V, and 65% continued to 450 V Milgram (1974).

Variations. Milgram continued to perform the experiment with 18 different variations to identify the factors that affect obedience Milgram (1974). The variations along with the results have been summarized in Table 15.

3.5.4. Commitment & Consistency

The offender first attempts to get the victim to make a small choice in his favor. Once the victim has complied, they become more likely to grant subsequent, larger requests, either to avoid cognitive dissonance[6] or because, as Self-Perception Theory proposes Bem (1972), people infer their own attitudes by observing their behavior. As a result, after agreeing to a small request, they begin to see themselves as "helpers" or "participants" and thus feel compelled to agree again in order to maintain that self-image. There are two main techniques that take advantage of the aforementioned behavior.

Foot-in-the-Door technique (FitD). FitD is a persuasive approach grounded in the principle of gradual commitment. At its core, this technique involves an initial outreach by the persuader with a modest and undemanding request. This introductory appeal is intentionally designed to be easily accepted by the respondent. Once the respondent complies with this initial request, the persuader then presents a subsequent, more substantial demand that aligns with their true objective. The psychological underpinning of this technique lies in the principle of consistency. The respondent's initial agreement creates a sense of cognitive dissonance, triggering a desire to maintain harmony between their actions and beliefs. Consequently, the respondent is more inclined to acquiesce to the subsequent, larger request as an extension of their prior commitment. The Foot-in-the-Door Technique adeptly capitalizes on the human propensity to align behavior with past actions, significantly heightening the prospect of achieving the persuader's ultimate goal. The technique has been analyzed by Jonathan L. Freedman and Scott C. Fraser Freedman and Fraser (1966), who performed two experiments.

In the first experiment Freedman and Fraser (1966), participant compliance rate was measured for N=36 participants under different conditions:

- **Performance:** Participants were asked to comply with a small request and 3 days later with a larger request that was related to the first.
- **One-Contact:** Participants were asked to comply only with the large request.
- **Agree-Only:** Participants agreed to the first request but did not carry it out (to measure if carrying out the request actually changes compliance rate).

[6] Mental discomfort caused by conflicting beliefs, behaviors or attitudes.

Table 15
The Milgram Experiment Variations

#	Alteration	Changes	% reached 450 V	Effect
1	The initial experiment	-	65%	-
Closeness of the Victim				
2	Voice-Feedback	Vocal Protest introduced.	62.5%	Slightly reduced obedience
3	Proximity	Victim visible in the same room.	40%	Moderately reduced obedience
4	Touch-Proximity	The victim was only shocked when resting their hand on a shock plate. From 150 V onward, the victim refused to comply and the experimenter ordered the "teacher" to force the victim's hand on the plate.	30%	Greatly Reduced obedience
Further Variations and Controls				
5	Different Location	Experiment was conducted in Yale's Basement, victim mentioned heart condition.	65%	No change
6	Change of Personnel	New unaggressive "experimenter" and dry, technical-looking "learner"	50%	Little effect
7	Closeness of Authority	Experimenter left the laboratory after initial instructions and gave orders by telephone.	20.5%	Greatly Reduced obedience
8	Women as Participants	More yielding than men yet less aggressive and more empathic according to Milgram.	65%	Incredibly higher conflict
9	Victim's Limited Contract	Both participants signed a general release form releasing Yale from any legal claims. The "learner" says they will agree on the condition that they will be let out when they say so, because of their heart condition. The "experimenter" grunts in a positive manner.	40%	The participants bring up the victim's conditions to their participation, lower obedience.
10	Institutional Context	Relocation to Bridgeport under the cover of "Research Associates of Bridgeport", therefore dissociating the experiment from Yale. Sparsely furnished and marginally respectable laboratory.	47.5%	Participants concerned about the legitimacy of the experiment, reduced obedience
11	Participant Chooses Shock Level	Experiment 5 but the "teacher" can choose any shock level.	2.5%	Immensely reduced obedience
Role Permutations				
12	Learner Demands to be Shocked	The "learner" demands to be shocked since a friend of theirs went through the entire experiment and the "experimenter" forbids shocking them due to the victim's heart condition.	0%	Deduction: It is not the command the participant is obedient to but the authority.
13	Ordinary Experimenter	Eliminating the status component of the "experimenter's" role but retaining the imperative to shock the victim. "Experimenter" appears to be a participant and supposedly comes up with the idea for the system to administer the shocks with enthusiasm.	20%	
13a	Participant as Bystander	After refusing to comply with the instructions of the common man, the man asserts that he will take over and administer the shocks himself and moves in front of the shock generator.	68.75%	All participants protest, some show hostility to common man and some restrain him physically.
14	Authority as Victim	The associate acts as a "learner" that is afraid of the shocks. The "experimenter" places himself as the receiver to reassure the associate initially given the "learner" role that the experiment is not dangerous. Participant still administers the shocks.	0%	
15	Two Contradicting Authorities	At 150 V when the "learner" protests, one "experimenter" gives the command to proceed but the second "experimenter" directs the opposite to the participant.	0%	All participants stopped exactly at the disagreement point (and one earlier). The participants tried to reconstruct hierarchy and determine which experimenter has higher authority.
16	Two Authorities, One as Victim	Two "experimenters", one of which gives the orders and the other fulfills the "learner" role.	65%	Having authority as a victim is no better than having no authority at all.
Group Effects				
17	Two Peers Rebel	The "teacher" participant has two peers (Milgram's associates), which stop participating at 150 V and 210 V respectively.	10%	Authority weakened because of non-compliance, defiance seems possible and natural and marking of the participant's actions as improper by their peers.
18	Peer Administers Shocks	The "teacher" participant has a peer (Milgram's associate) that performs the task of using the lever of the shock generator, while the participant reads the words.	92.5%	The participant is distanced from the actual act of brutality, and is very likely to comply.

- **Familiarization:** Participants were given as much familiarity as the performance and agree-only conditions without any request being made to them (to measure if being familiarized with the experimenter is the cause that might increase compliance rate upon a second request).

The results can be summarized in Table 16 and Figure 18, where significance levels reflect changes with respect to the performance scenario. The experimental condition shows a higher compliance rate. Actually carrying out the small request increased the compliance of the participants on the large request as seen from the performance condition, which is considerably higher than the agree-only condition.

In the second experiment Freedman and Fraser (1966), participant compliance rate was measured for 105 women and 7 men living in Palo Alto, California. Contact with all participants was made between 1:30 and 4:30 in the afternoon between Monday-Friday. A small request was made to the participants which could be one of the four issues:

- Putting up a small sign for safe driving.

Table 16
Results of the Foot-in-the-door Experiment 1

Condition	Performance (FitD)	Agree-Only	Familiarization	One-Contact
Compliance %	52.8% (19/36)	33.3% (12/36)	27.8% (10/36)	22.2% (8/36)

Note: The significance levels of other conditions compared to Performance are the following: Familiarization, $p < .07$; One-Contact, $p < .02$.

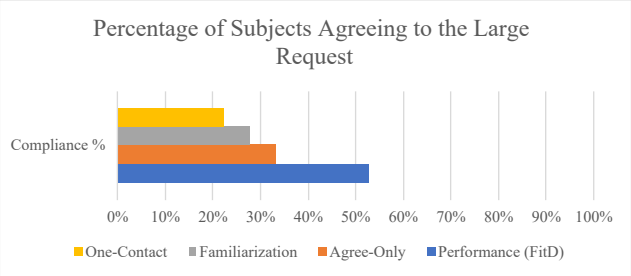

Figure 18: Compliance using Foot-in-the-Door Technique (Experiment 1)

Table 17
Results of the Foot-in-the-door Experiment 2

	Similar Task	Different Task
	Safe Driving Sign	Safe Driving Petition
Similar Issue	**76% (19/25)**	47.8% (11/23)
	Beauty Sign	Beauty Petition
Different Issue	47.6% (10/21)	47.4% (9/19)
One-Contact: 16.7%		

- Putting up a small sign for beauty.
- Signing a petition for safe driving (with at least 20 signatures already on).
- Signing a petition for beauty (with at least 20 signatures already on).

After 2 weeks from the first contact, all participants were contacted again, and asked if they would put a large sign regarding safe driving in their front yard, reading "Drive Carefully", for a week or a week and a half (task). They were also shown a picture of the sign and informed that the mounting process would be the experimenters' responsibility and would cause no damage to their lawn. The control group was simply asked to put a large sign on their lawn.

The first request increased the compliance rate of the second request when it was a similar task to the second, as shown in the results in Table 17 and Figure 19.

Low-Ball technique. Operating in tandem with the principle of commitment and consistency, the Low-ball Technique is a strategic method of persuasion that plays on psychological dynamics. This technique commences with the persuader presenting an alluring offer to the respondent, often at an

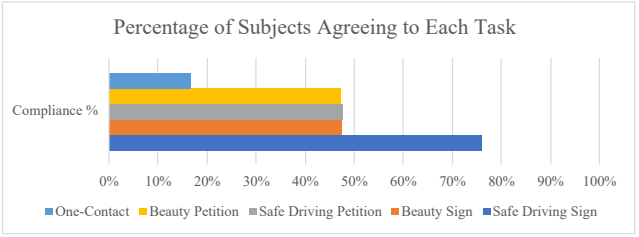

Figure 19: Compliance using Foot-in-the-Door Technique (Experiment 2)

unusually affordable price point. This initial proposal captures the respondent's attention and engenders a sense of enthusiasm, prompting them to express an initial agreement. However, following the respondent's affirmation, the persuader discloses previously concealed costs, terms, or limitations that result in a modification of the deal, rendering it less favorable than initially perceived. Remarkably, despite the alterations, the respondent is more likely to honor their original commitment and proceed with the agreement. This curious phenomenon arises because the act of agreeing to the initial offer establishes a psychological commitment within the respondent's mindset. This, in turn, motivates them to rationalize their continued participation based on the pursuit of consistency between their actions and convictions. The Low-ball Technique astutely leverages this inherent human inclination, exploiting the cognitive dissonance that arises to effectively secure compliance and steadfast commitment from the respondent. Cialdini Cialdini, Cacioppo, Bassett and Miller (1978) performed three different experiments to study this technique.

The first experiment was performed on 63 participants who were enrolled in introductory psychology classes. The participants were told either of the following:

- "The room in which the experiment is being held is used during the day and evening by other people in the department; so we are running this experiment at 7:00 in the morning on Wednesdays and Fridays. Can I put you down for Wednesday or Friday morning at 7:00?".
- Partially described the experimental requirements, omitting the time, and using "Well, we have more than one time during the week, but right now I'm just interested in finding out if you wish to participate" in case the participant asked about the time.

The results of the experiment can be summarized in Table 18 and Figure 20, which show not only that the low-ball technique was superior for initial compliance of the participants but also improved the rate of commitment of the participants (i.e. the rate of participants that turned up from the participants that initially complied).

In the second experiment 30 male graduate students who lived in the dorms of a large state university were contacted by an experimenter. The experimenter's request was to get the students to agree in putting up some posters that they

Table 18
Results of the Lowball Experiment 1

	Initial Compliance	Turn-up	Commitment
Control Condition	31% (9/29)	24% (7/29)	79% (7/9)
Low-Ball Condition	56% (19/34)	53% (18/34)	95% (18/19)

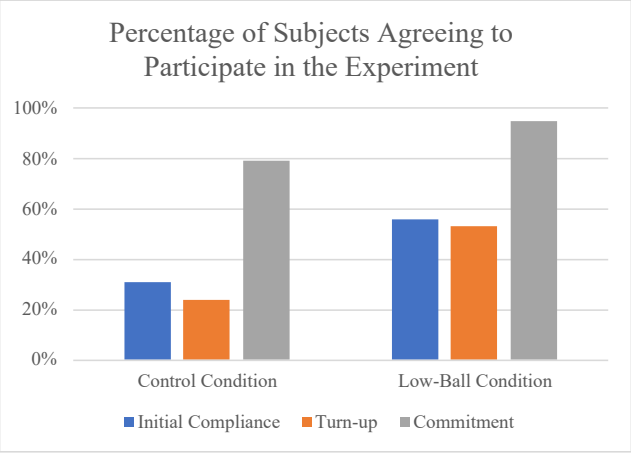

Figure 20: Compliance using Low-Ball Technique (Experiment 1)

Table 19
Results of the Lowball Experiment 2

	Initial Compliance	Turn-up	Commitment
Control Condition	70% (7/10)	20% (2/10)	28.6% (2/7)
Low-Ball Condition	80% (8/10)	60% (6/10)	75% (6/8)
FitD Condition	70% (7/10)	10% (1/10)	14.3% (1/7)

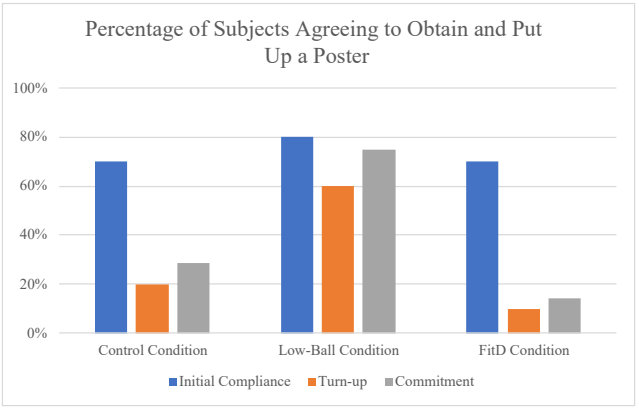

Figure 21: Compliance using Low-Ball Technique (Experiment 2)

would obtain from the dorm desk within one hour from initial contact. Two different conditions were studied:

- **Control Condition:** Participants learned that they will need to get a packet of posters from the dorm desk downstairs within one hour, and then they were asked if they would be willing to put up the posters.
- **Low-Ball Condition:** Participants were first requested to display the posters. In case they agreed, they were informed that they would have to obtain the posters within an hour, and then asked again if they could put up the posters by the experimenter.
- **Foot-in-the-door condition:** Participants were asked if they would put up a window poster that the experimenter carried, and then requested to go to the downstairs desk within the same hour to get a door poster that the experimenter supposedly ran out of.

This experiment, similar to the second experiment, shows that the low-ball technique might have been superior for initial compliance of the participants and greatly improved the rate of commitment of the participants as well. The results of the experiment are summarized in Table 19 and Figure 21.

In the third experiment the participants were 144 students (both male and female) enrolled in an introductory psychology course. The course required four hours of participation experiments during the term. The experiment was described to them to be about their opinion on two different personality tests. The following conditions were tested:

- **Low-Ball Condition:** After rating the personality tests, participants read that they would get twice the credit for taking one of the two tests, due to the experimenter needing more respondents for it. The participants were then:
  - Allowed to change their decision (high volition)
  - Assigned to take the test with the most credit (low volition)

  After the tests were re-rated, the experimenter informed the students that the statement for twice the credit was an error, and both tests gave the same credit. Then the participants were allowed to change test for their final selection.
- **Control Condition:** Participants were not aware of any differences in experimental credit gained for each test, and were allowed to change their decision after selecting in order to have identical conditions with the low-ball condition.

The participants were given a questionnaire after this process regarding the following points:

- Whether or not the final selection of the test was their own choice
- How they would estimate they and their peers would score on the tests
- Any hypotheses or suspicions regarding the experiment

Table 20
Results of the Lowball Experiment 3

	Initial Sel. of Target Test	Final Sel. of Target Test	Commitment
Low-Ball (high volition)	81% (39/48)	61% (29/48)	74% (29/39)
Low-Ball (low volition)	Assigned (48/48)	42% (20/48)	42% (20/48)
Control Condition	31% (15/48)	31% (15/48)	100% (15/15)

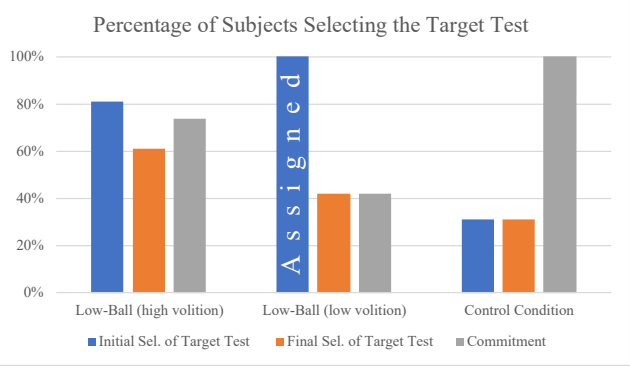

Figure 22: Compliance using Low-Ball Technique (Experiment 3)

This experiment, similar to the previous experiments, shows that the low-ball technique is superior to the control condition for initial compliance of the participants (81% vs 31%, $p < .001$). Despite the decline in commitment compared to the participants' control condition decision, the final selection rate for the target test was significantly higher (61% vs 31%, $p < .005$). The results are summarized in Table 20.

3.5.5. Liking

The offender behaves in a way that seems friendly and nice, such as giving compliments to the victim. The offender can also lie about their personal habits and tastes to match with the victim's, therefore giving a sense of likeability and similarity to the victim Bullée et al. (2018). There are several ways for an offender to gain additional advantage by how the victim views them Cialdini (2007):

- **Physical Attractiveness:** People assign favorable traits like talent, kindness, honesty and intelligence to attractive individuals.
- **Similarity:** People are more likely to help someone dressed like them, or having similar background and interests.
- **Compliments:** An experiment done in North Carolina where the participants received comments about them by a person who needed a favor showed that Cialdini (2007):
  - The participants liked the person that gave only praise best.
  - The participants continued to do so even when they realized the person wanted something in return.
  - The comments did not have to be accurate or true for the participants to comply.
- **Contact and Cooperation:** Familiarity is an important factor to an individual's choice. In the past, exposure between groups has been proposed as a way to improve race relations, since being exposed to the same thing in the past makes an individual like it more. On the contrary, psychologist Elliot Aronson who tried this approach in Austin, Texas ended up with a classroom full of hatred Aronson, Blaney, Stephan, Sikes and Snapp (1978). The students were each given only one piece (of the puzzle) of information needed to pass the test. This technique is known as "the Jigsaw Classroom" and has been used ever since as a learning technique. The task at hand could only be accomplished if everyone cooperated, and thus the imposition of common goals between the students was what brought them back together, and turned former enemies into valuable friends.
- **Conditioning and Association:** The offender can utilize the conclusions from Pavlov's experiment to create an association between them and something that naturally produces a certain behavior of the victim. For example, food (unconditioned stimulus - UCS) produces a positive behavior (unconditioned response - UCR). The offender, who has associated themselves with food (conditioned stimulus - CS), invokes a similar response (conditioned response - CR) to that of food for the victim. The conditioned and unconditioned responses are the same, but are triggered by different stimuli. The classical conditioning process can be summarized in Figure 23.

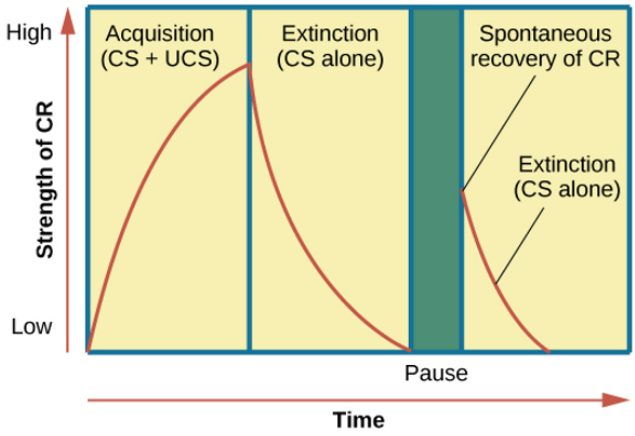

Figure 23: Classical Conditioning

The Chameleon Effect. Besides Cialdini's techniques for gaining likeability, the chameleon effect is also worth considering. The chameleon effect occurs when an individual nonconsciously mimics postures, mannerisms, facial expression of their interaction partners. It has been shown that said mimicry makes interactions smoother as well as increases

Table 21
Results of the Chameleon Effect Experiment

	Liking	Smoothness
Mimicking	M = 6.62	M = 6.76
No Mimicking	M = 5.91	M = 6.02

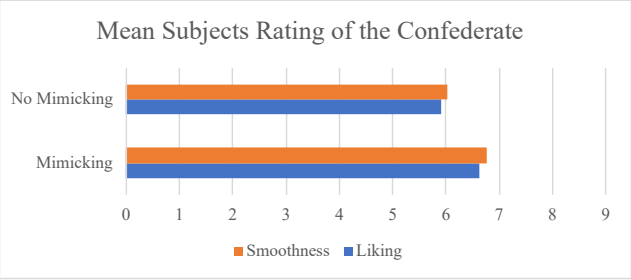

Figure 24: The Effectiveness of the Chameleon Effect on Liking and Smoothness

the liking between the people interacting Chartrand and Bargh (1999). During a 15-minute session, the participants and the experimenter's confederates took turns describing what they saw in photographs. Confederates either mirrored the mannerisms of the participant (experimental condition) or performed neutral mannerisms (control condition). The participants were then asked to report how much they liked the confederate and how smoothly the interaction went on a scale from 1 (extremely awkward) to 9 (extremely smooth/likable). The results of the experiment can be summarized in Table 21, as well as in Figure 24.

It is interesting to note that only 1 out of 37 participants noticed the confederate's similar mannerisms, but did not realize it was a result of mimicking, saying "it seemed normal". It has been noted that interpersonal closeness also leads to mimicking. This means that mimicking increases interpersonal closeness, which then increases mimicking, causing a cycle Lakin, Jefferis, Cheng and Chartrand (2003). This further amplifies the potential of this technique in social engineering.

3.5.6. Conformity

There are a total of 4 types of Conformity defined over the years, which include Saul (2023b):

- Three (3) types of conformity distinguished Kelman (1958):
  - **Compliance:** An individual accepts influence in order to get a favorable reaction from a person or group, and avoid disapproval. It is possible for the individual to decline.
  - **Internalization:** An individual accepts influence for the intrinsic rewards (inherent satisfaction and not external reward). It includes the feeling of accomplishment from beating challenges, satisfying one's curiosity, having a sense of control and understanding the context and utility of knowledge in real-life situations (Nickerson, 2021).
  - **Identification:** An individual accepts influence in order to establish or maintain a self-defining relationship to another person or group, such as the guards in the Stanford Prison Experiment which immediately conformed to their role in the experiment.
- An additional type identified by Mann Mann (1969):
  - **Ingrational:** An individual accepts influence solely to gain acceptance, and peer pressure does not influence their decision to conform.
- There have been two (2) explanations in regards to why people conform Saul (2023b):
  - **Normative Conformity:** An individual wants to fit in with a group, and has the fear of being rejected. Usually, the individual does not privately accept the views of the group, even though they publicly accept them.
  - **Informational Conformity:** An individual is unsure regarding the decision at hand and looks to the group for guidance. The individual accepts and internalizes the views of the group.

4. Implementation of Psychological Techniques in Real-life Phishing Attacks

To achieve this, we first performed exhaustive research across established search engines (e.g. Google, Bing, DuckDuckGo) using targeted keywords such as "notable phishing attacks", "phishing email attacks", and "phishing incidents". For each identified attack, we then determined which psychological techniques from our taxonomy were employed. After conducting a thorough review of documented cyberattacks from reputable sources (including government reports, legal documents, cybersecurity threat intelligence platforms, and major news outlets), the studied incidents were selected based on the following criteria:

- The incidents are well-documented in public reports, legal findings, and cybersecurity analyses.
- The incidents represent massive financial losses and data leaks.
- The targets constitute large organizations spanning various industries (e.g., technology, manufacturing, pharmaceuticals, government).
- The incidents demonstrate the use of sophisticated psychological manipulation techniques and are representative of the cases studied.

Notable incidents such as the DocuSign phishing campaign (2017)[7], British Airways breach (2018)[8], Twitter Bitcoin scam (2020)[9], Axie Infinity breach (2022)[10], and CircleCI phishing attack (2023)[11] were excluded because they either did not align with one or more of these criteria or did not offer additional value to the analysis. As the study aims to investigate the effectiveness of the techniques, incidents are reported in ascending order of financial damage caused by the attack.

In 2016, Snapchat faced a phishing email attack that exploited the *Authority* psychological method (described in section 3. The target was an HR employee, and the attacker pretended to be the CEO (Authority), asking about asking about employee payroll information. This resulted in a leak of sensitive employee data Daly (2021) that fall under Personally Identifiable Information (PII) according to the Department of Labor U.S. Department of Labor.

Speaking of the Department of Labor (DoL), in January 2022, it faced a phishing attack using the techniques *Authority*, *Reciprocity* and *Scarcity*. The attackers imitated the DoL (Authority) to send emails asking recipients to submit their bids on a government project (Reciprocity) in an urgent manner (Scarcity). The recipients were redirected to a Microsoft Office 365 email login page after clicking the bid button, which stole their credentials Toulas (2022b); Tessian (2023).

In 2019, an unnamed UK-based energy firm received a vishing attack (similar to phishing but via phone) using the *Authority* technique. The CEO received a phone call from an individual that sounded exactly like his boss (Authority), who was the chief executive of their parent company. The audio was constructed using deepfake technology, using AI to construct speech samples segments on existing speech samples. The CEO was instructed to transfer 243 thousand dollars to a fraudulent account that was allegedly a Hungarian supplier. This case showcases how advanced technology can be used in cybercrime.

In 2016, an aerospace parts manufacturer "FACC" faced a phishing attack using the *Authority* technique and suffered a loss of 42 million dollars when the attackers studied the CEO's writing habits and impersonated his writing style (Authority) to request fund transfers from employees in the finance department TrendMicro (2016); Lichumon (2023); Purohit (2022).

In 2015, a US-based tech company "Ubiquiti Networks" was defrauded 46.7 million dollars through spear-phishing using the *Authority* technique. The perpetrators impersonated company executives (Authority), in order to trick employees into transferring funds to accounts they controlled Daly (2021); Lichumon (2023); Purohit (2022).

In 2014, a US drug company "Upsher-Smith Laboratories" faced a phishing attack employing the *Authority* technique and lost over 50 million dollars. The attack boiled down to a CEO impersonation scam (Authority) that convinced the accounts payable department to perform a series of fraudulent wire transfers Purohit (2022).

Perhaps the most prominent and high-profile case of corporate fraud is the 100 million dollar Google and Facebook Spear Phishing Scam, that employed *Authority*, *Reciprocity*, *Commitment & Consistency* and more specifically the *Foot-in-the-door (FitD)* approach. This scheme started in 2013 and went on for 2 years. The perpetrator set up a fake computer with a name that resembled a company that was a known hardware supplier to Google and Facebook (Authority). Using forged email addresses that appeared to be from the newfound company, the attackers sent emails to request payments for non-existent supplies and services (Reciprocity). This process was carried out repeatedly for the duration of the attack (Commitment & Consistency, FitD)Department of Justice (2019); Tessian (2023); Lichumon (2023); Purohit (2022); Daly (2021). Table 22 highlights the techniques employed in each of the most notable phishing attacks that have occurred while Figure 25 provides a timeline of studied attacks.

It is clear that in most cases, social engineering attacks employ some form of Authority to maximize their success rate, especially as the initial technique. This aligns with the findings of Bullée et al. (2018), where the authors analyzed four social engineering books written by social engineers and found that the Authority technique was used in 76 (53.5%) of all 142 documented attack steps. Authority was always one of the two techniques employed when multiple techniques were used simultaneously (27 occurrences). Moreover, from their analysis, we can deduce that Authority was used as the first step (alone or in combination with other techniques) in 56 (75.7%) of the 74 scenarios and as the last step in 29 (82.9%) of the 35 multi-step scenarios. At least one psychological technique was involved in each notable example, and some attacks combined multiple techniques for added effect. Remarkably, the most financially damaging case, involving Google and Facebook, utilized three of the most potent persuasion principles identified by Cialdini Cialdini (2007).

5. Effectiveness Metrics, Comparison and Validation

This section delves into an in-depth analysis of the effectiveness of various psychological techniques commonly employed in online social engineering attacks. A comprehensive approach is proposed to evaluate the potency of these techniques, combining novel metrics introduced in this article. This comparative analysis sheds light on the strengths and weaknesses of each technique, providing valuable guidance for researchers and practitioners in both cybersecurity and psychology.

[7] DocuSign (2017); Krebs (2017)

[8] Source Defense (2022); BBC News (2018, 2019, 2020a)

[9] Tessian (2023); New York Department of Financial Services (2020); Mitnick Security (2020); BBC News (2020b)

[10] Tidy (2022); Sigalos (2022); Toulas (2022a); Votiro (2022)

[11] AO Labs (2023); Perception Point (2023)

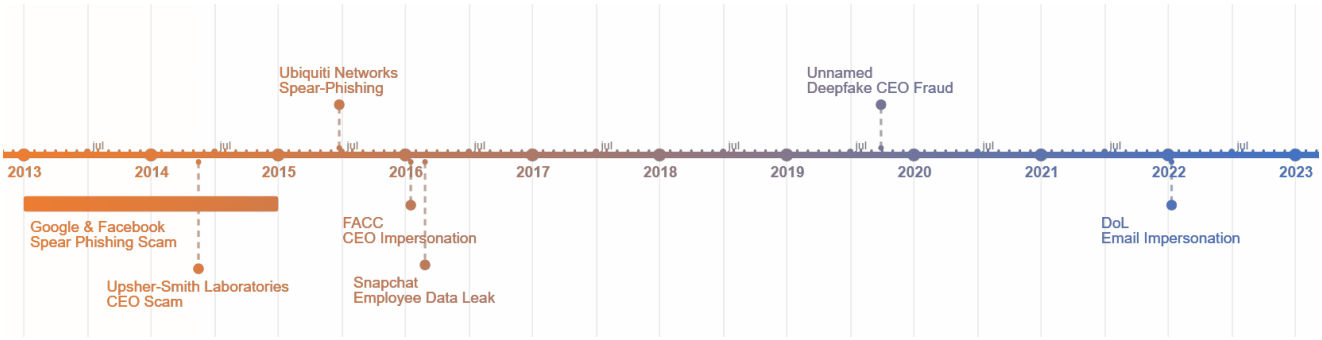

Figure 25: A timeline of the studied real-world phishing attacks

Table 22
Psychological Techniques Employed in Real-Life Phishing Attacks

Phishing Attack	Year	Psychological Technique Used	Financial Impact
Snapchat Employee Data Leak	2016	Authority	N/A
DoL Email Impersonation	2022	Authority → Scarcity → Reciprocity	N/A
Deepfake CEO Fraud	2019	Authority	$ 243k
FACC CEO Impersonation	2016	Authority	$ 42M
Ubiquiti Networks Spear-Phishing	2015	Authority	$ 46.7M
Upsher-Smith Laboratories CEO Scam	2014	Authority	$ 50M
Google and Facebook Spear Phishing Scam	2013-2015	Authority → Commitment & Consistency: FitD → Reciprocity	$ 100M

The proposed metrics represent a significant advancement in evaluating psychological techniques in social engineering. They enable a systematic and quantitative assessment of individual methods and offer a novel framework for comparing techniques across diverse scenarios—a contribution largely absent in prior literature. These metrics are highly applicable, balancing real-world insights with proportional effectiveness and providing a holistic perspective that mitigates the limitations of individual measures. Their introduction lays a foundation for future studies to adopt more rigorous and standardized approaches in assessing compliance and conformity techniques, thereby enhancing reproducibility and standardization in this field.

5.1. Defining Effectiveness Metrics

Based on the analysis of the psychological techniques, this article introduces two primary metrics to gauge their effectiveness in enhancing the success rate of social engineering attacks: the Absolute Compliance Increase Rate (ACR) and the Relative Compliance Increase Rate (RCR). Given that the primary metrics have their strengths and weaknesses, the Comprehensive Compliance Increase Rate (CCR) is proposed, taking into account both primary rates to combine their strengths and mitigate their biases. Below is a detailed description of each metric along with its inherent advantages and drawbacks.

When referring to Compliance Rates (CRs), note that:

- **Post-technique CR** is the compliance rate using the respective psychological technique (experimental condition).
- **Pre-technique CR** indicates the initial compliance rate without the introduction of the technique (control condition).

Absolute Compliance Increase Rate (ACR). This metric directly measures the change in compliance between the pre-application and post-application of a technique, without accounting for relative starting points.

The formula for this metric is defined as:

$$\text{ACR}\ (\%) = \text{Post-technique CR} - \text{Pre-technique CR} \quad (1)$$

Pros:

- **Intuitive Understanding**: This metric offers a direct and easily comprehensible comparison. For example, an increase from 40% to 50% is a 10% absolute increase.
- **Volume Insight**: Provides a clear picture of the raw number of individuals who became compliant due to the technique.

Cons:

- **Baseline Ignorance**: The metric does not factor in initial compliance rates. For example, a compliance increase from 5% to 15% is a greater relative shift (200% relative increase) than going from 40% to 80% (100% relative increase), even though the absolute increase is quadruple.
- **Potential Misleading Comparisons**: In instances where starting compliance varies significantly between studies, this metric might present skewed comparisons.

Relative Compliance Increase Rate (RCR). This metric measures the proportionate increase in compliance, thus providing insights into the technique's effectiveness relative to its starting compliance rate (CR).

The formula for this metric is defined as:

$$\text{RCR } (\%) = \left(\frac{\text{Post-technique CR} - \text{Pre-technique CR}}{\text{Pre-technique CR}} \right) \times 100 \tag{2}$$

Pros:

- **Baseline Consideration**: By comparing growth rates, this metric acknowledges and emphasizes the impact of techniques that might triple compliance, for instance, from 5% to 15%.
- **Normalized Comparisons**: Especially beneficial in our study where initial compliance rates differ across techniques, this metric offers a harmonized comparison platform.

Cons:

- **Extreme Ends Deception**: At the spectrum's ends, the metric can overemphasize growth; for instance, a jump from 1% to 2% is a 100% increase but remains marginal in absolute terms.
- **Volume Ambiguity**: The metric doesn't inherently illustrate the total number of individuals impacted.

When assessing techniques that have been tested in multiple experiments, it is imperative to compute average values to gain a clear perspective on their efficacy.

- For the Absolute Compliance Rate (ACR)

  Given ACR_i as the Absolute Compliance Rate of the ith experiment and considering N experiments, the average ACR can be represented as:

$$\text{Average ACR} = \frac{1}{N} \sum_{i=1}^{N} \text{ACR}_i \tag{3}$$

- For the Relative Compliance Rate (RCR):

  Given RCR_i as the Relative Compliance Rate for the ith experiment and considering N experiments, the average RCR is expressed as:

$$\text{Average RCR} = \frac{1}{N} \sum_{i=1}^{N} \text{RCR}_i \tag{4}$$

Such averaging ensures a more comprehensive and balanced view of each technique's effectiveness, considering all conducted experiments.

To achieve a comprehensive understanding of the techniques' effectiveness, our analysis integrates insights from both metrics. While the relative rate grants us clarity on the technique's potency, the absolute rate elucidates its broader, real-world implications. This dual metric approach ensures a balanced evaluation, addressing both the depth of the technique's impact and its breadth in a wider context.

Comprehensive Compliance Increase Rate (CCR). For a holistic perspective on the efficacy of psychological techniques in driving compliance, the Comprehensive Compliance Increase Rate (CCR) is introduced. This rate amalgamates the insights from both the Absolute and Relative Compliance Increase Rates, attributing equal weights to each. Formally, the CCR can be represented as:

$$\text{CCR} = \frac{1}{2}(\text{Average RCR} + \text{Average ACR}) \tag{5}$$

The CCR is conceived to harness the strengths of both the absolute and relative metrics, enabling a balanced approach and encompassing evaluation of each technique's impact on compliance.

Normalized Comprehensive Compliance Increase Rate (nCCR). To further enhance the utility and interpretability of the CCR, a normalized version is introduced, denoted as nCCR. This normalized metric retains the relative effectiveness between different techniques while constraining the values within a bounded range of [-1, 1]. It is thus not only aiding in preserving the essential characteristics of the data but also facilitates a more direct comparison of different compliance techniques. The normalization is achieved through the following mathematical representation:

$$\text{nCCR} = \frac{\text{CCR}}{\max\left(\left|\text{CCR}_{\max}\right|, \left|\text{CCR}_{\min}\right|\right)} \tag{6}$$

Where:

- $\text{CCR}_{\max}$ is the maximum observed CCR value in the dataset.
- $\text{CCR}_{\min}$ is the minimum observed CCR value in the dataset.

Table 23
Principles & Techniques Effectiveness Comparison

Technique Name	$CR_{initial}$	CR_{final}	ACR	RCR	≈RR†	CCR	nCCR	Notes
Majority Size	8.60%	34.25%	25.65%	298.26%	3.98	1.619529	1	Majority size 1,2 average vs 3,4,6,7,9,15 average.
AUTHORITY	20.00%	66.72%	46.72%	233.60%	3.34	1.4016	0.865	Initial Compliance calculated from the average of variations 11,13. Final Compliance calculated from the average of variations 1,2,5,6,8,13a,16,18.
COM: Foot-in-the-Door (FitD)	19.45%	64.40%	44.95%	231.11%	3.31	1.380277	0.852	
COMMITMENT & CONSISTENCY	22.23%	61.20%	38.98%	175.37%	2.75	1.071703	0.662	
COM: Low-Ball	25.00%	58.00%	33.00%	132.00%	2.32	0.825	0.509	
REC: That's-not-All technique (TNA)	37.08%	72.03%	34.95%	94.27%	1.94	0.646092	0.399	In case of Negotiation and No-negotiation TNA conditions the Negotiation Condition was selected
RECIPROCITY	32.12%	62.61%	30.49%	94.93%	1.95	0.627098	0.387	
REC: Door-in-the-Face technique (DitF)	27.17%	53.20%	26.03%	95.83%	1.96	0.609308	0.376	Smaller-request-only and Rejection-moderation conditions were selected for Initial and Final Compliance
Congruity (High Status)	32.00%	55.00%	23.00%	71.88%	1.72	0.474375	0.293	
Real Information (Large Favors)	24.00%	42.00%	18.00%	75.00%	1.75	0.465	0.287	
Real Information (Small Favors)	60.00%	94.00%	34.00%	56.67%	1.57	0.453333	0.280	
COM: Request Similarity	47.60%	76.00%	28.40%	59.66%	1.60	0.440319	0.272	
Placebic Information (Small Favors)	60.00%	93.00%	33.00%	55.00%	1.55	0.44	0.272	
Real Information	42.00%	68.00%	26.00%	61.90%	1.62	0.439524	0.271	
Unanimity	63.00%	89.00%	26.00%	41.27%	1.41	0.336349	0.208	One participant vs 2 allied participants
LIK: Chameleon Effect	59.65%	66.90%	7.25%	12.15%	1.12	0.097021	0.060	
Placebic Information (Large Favors)	24.00%	24.00%	0.00%	0.00%	1.00	0	0	
Congruity (Random Status)	37.00%	20.00%	-17.00%	-45.95%	0.54	-0.31473	-0.194	

† Risk Ratios (RRs) can be recovered from RCR as:

$$RR = \frac{\text{Post-Technique CR}}{\text{Pre-Technique CR}} = \frac{\text{Post-Technique CR}}{\text{Pre-Technique CR}} - 1 + 1 = \frac{\text{Post-Technique CR} - \text{Pre-Technique CR}}{\text{Pre-Technique CR}} + 1 = \frac{\text{RCR\%}}{100} + 1 \tag{7}$$

Employing nCCR allows for a nuanced evaluation that is grounded in the robust analytical foundation provided by the CCR while enhancing the comprehensibility and ease of analysis. It serves to ensure that the graphical representation of the effectiveness of different techniques maintains the original distribution shape, thus providing a realistic and undistorted perspective on the comparative strengths of various strategies in enhancing compliance. It is crucial to note that this normalization is context-specific; if additional techniques were to be introduced into the dataset, the nCCR must be recalculated to account for potential changes in CCR_{max} and CCR_{min}.

5.2. Effectiveness Comparison and Validation

A comprehensive summary of the psychological techniques, along with their effectiveness metrics, is presented in Table 23. In addition to our custom nCCR metric, we have computed an approximate Risk Ratio (RR) for each technique. These RRs provide an intuitive multiplier of compliance likelihood (e.g., RR = 3 means "three times more likely to comply"). Because Table 23 entries are aggregated percentages from studies with varying sample sizes—and in some cases only percentages were available—these RRs should be regarded as descriptive approximations rather than precise inferential estimates. Notably, the ordering of the techniques by nCCR is nearly identical to that obtained using RR. To quantify this agreement, we computed Spearman's rank-order correlations between nCCR and RR, $\rho = .975, p < .001$, and between absolute compliance gains (ACR) and RR,$\rho = .624, p = .006$. This strong concordance provides additional validation that our composite nCCR metric captures the same underlying effect-size signal as conventional risk-ratio estimates.

Figure 26 illustrates the techniques' effectiveness based on the nCCR data from Table 23, enabling a comparative

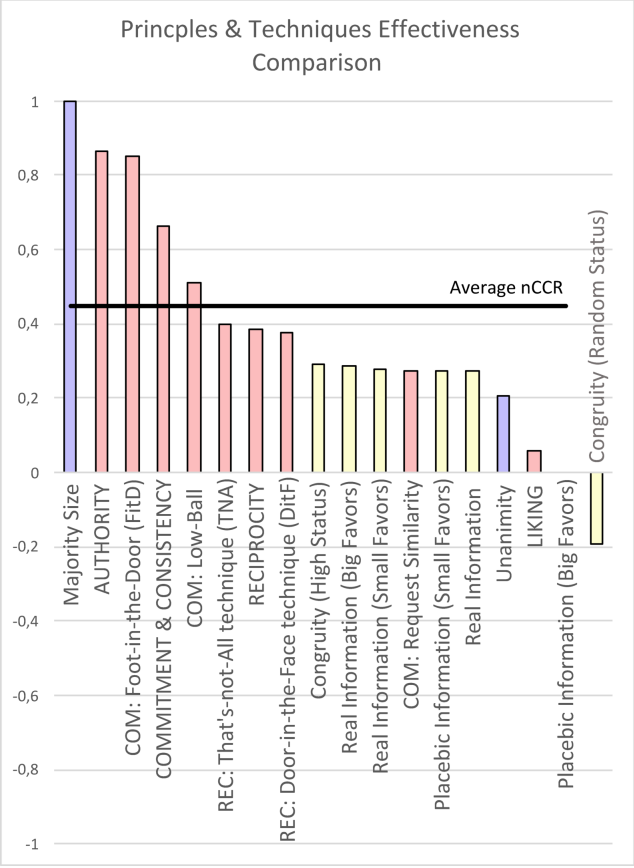

Figure 26: Principles & Techniques Effectiveness Comparison based on nCCR

Table 24
Comparison between the Principle Effectiveness Rating between this article and Bullée et al. (2018)

Principle	nCCR	Compliance Rating by Bullée et al. (2018)
Authority	0.86	62.5%
Commitment & Consistency	0.66	45.2%
Reciprocity	0.39	41.1%

analysis of Cialdini's principles. In Bullée et al. (2018), a similar comparison was conducted using 74 scenarios extracted from four social engineering books authored by social engineers. For validation, the results of this article were compared with those of Bullée et al. (2018), and the alignment between these findings is shown in Table 24, which highlights the consistency in ranking and ratings observed across both works.

It is interesting that the ranking of the principles in terms of effectiveness from Bullée et al. (2018) based on social engineering books matches the ranking of techniques calculated by our research based on psychological experiments. This validates the results of the literature, pinpoints the potency of each principle of persuasion and confirms the hypothesis that these principles and techniques are the core of social engineering attacks.

6. Discussion, Limitations and Future Research Directions

This section discusses the key findings, limitations of the study, and future research directions to enhance our understanding of social engineering tactics and bolster defense strategies.

6.1. Discussion

In the discussion of the findings, it becomes evident that certain psychological principles consistently emerge as potent tools in the social engineer's arsenal. Authority stands out as a highly effective principle, which is supported by previous research and further validated in this study. These findings align with the observations from Bullée et al. (2018), which emphasize the prominence of authority in social engineering tactics, especially as the first or last technique when used in conjunction with other techniques in multiple contacts. The full potential of the Chameleon Effect is in effect when applied for a time frame to take advantage of the cycle of mimicking that increases interpersonal closeness, which then increases mimicking, causing a cycle Lakin et al. (2003). The effectiveness of this technique would scale well with the amount of contact and the duration of the attack.

Additionally, the majority size technique proves to be remarkably effective, especially in scenarios where the initial compliance rate is low. This technique's effectiveness can be attributed, in part, to the phenomenon of extreme ends deception. It excels in raising compliance rates from a low baseline to around 30%, underscoring its potential as a potent tool for social engineers. Interestingly, even when participants made almost no other mistakes (with a mere 0.54% error rate), they succumbed to the pressure of the majority. This suggests that the majority size technique can be particularly effective in situations where the victim's initial compliance is minimal, making it a valuable choice for social engineers aiming to exploit low base compliance levels. However, it may not be as effective when attempting to further raise compliance in situations where individuals are already reasonably compliant.

Proposing and utilizing novel metrics allows for a comprehensive evaluation of these techniques' effectiveness in diverse scenarios. The findings emphasize the significance of understanding the baseline compliance level when selecting the most suitable technique for a specific situation. Techniques with high Absolute Compliance Rate (ACR) are advantageous when working with a reasonable baseline, capitalizing on already-existing compliance tendencies. Conversely, techniques with high Relative Compliance Rate (RCR) shine in situations with low initial compliance, where they can induce substantial relative increases. When we translate the compliance gains into conventional risk ratios, the top techniques stand out particularly powerful. For instance, the Majority-Size and Authority cues both yield RRs approaching 4.0; meaning participants are nearly four times more likely to comply after those interventions. In behavioral science, RRs of 2.0 are typically seen as medium

effects, while RRs of 4.0 or higher qualify as very large effects Cohen (2016); Ferguson (2016). This underscores that the social-engineering principles that seem most effective by nCCRs also represent robust, real-world-sized impacts. These insights not only enhance the comprehension of social engineering tactics but also offer valuable guidance to security practitioners in selecting and deploying countermeasures tailored to the specific compliance landscape they aim to address.

To reduce individual susceptibility, organizations should implement continuous and engaging security—awareness programs, combining simulated phishing exercises, gamified training modules, and periodic refresher training sessions—to build employees' skills at identifying and resisting common social-engineering ploys Aldawood and Skinner (2019); Alshaikh (2020). At the collective level, fostering a strong information-security culture is critical: visible leadership support for cybersecurity, clear verification policies (e.g. secondary confirmation for unusual requests), and a non-punitive reporting environment encourage employees to question suspicious interactions rather than comply reflexively Flores and Ekstedt (2016); Nwankpa and Datta (2023). These individual-level and organization-level measures form a multilayered defense that directly targets the cognitive biases exploited by attackers in digital contexts.

6.2. Limitations

Understanding the limitations of this research is crucial to contextualize its findings and identify areas for improvement. While the study provides valuable insights into psychological techniques in social engineering, several constraints warrant consideration.

Controlled Experimental Settings. The experiments considered in this article face inherent constraints. Many experiments involve controlled settings with relatively small sample sizes, which may not fully capture the complexities of real-world social engineering scenarios. Additionally, the cultural and contextual factors that can influence the effectiveness of these techniques may not be fully addressed in the selected experiments. Future research should aim to conduct more extensive and diverse studies to validate and generalize the findings.

Real-World Context and Dynamics. A further limitation lies in reliance on controlled experiments, which may not fully encompass the breadth of social engineering tactics employed in practice. Real-world social engineering attacks often involve a combination of techniques, used in different order or in a single step, and attackers frequently adapt their strategies based on evolving trends and technologies. Consequently, the effectiveness of psychological techniques in isolation may not fully represent their real-world impact. Future research could explore more holistic and dynamic approaches, such as analyzing the interplay between multiple techniques and considering the influence of evolving technologies on social engineering. Beyond experimental settings and real-world dynamics, the tools for measuring effectiveness themselves present limitations.

Quantitative vs Qualitative Measures. The quantitative metrics introduced in this study, while valuable for systematically comparing techniques, inherently capture only a limited view of social engineering's complexity. They describe the relationship between a one-time application of a technique and compliance rates, potentially overlooking non-linear effects. These might include diminishing returns with repeated use or exponential impacts under certain conditions. Moreover, focusing solely on compliance rates does not incorporate participants' reasoning or long-term behavior. These qualitative aspects could provide a richer understanding of the techniques' effectiveness. Additionally, differences in offline and online settings pose further challenges.

Online vs. Offline Contexts. Because many psychological experiments are conducted offline, the derived effectiveness metrics may not accurately reflect the true impact of psychological techniques in online environments. In digital contexts, where physical cues such as body language, facial expressions, tone of voice, and situational context are absent, techniques may play out differently. These cues are often pivotal in establishing trust, conveying authority, and reinforcing message authenticity. Moreover, the asynchronous nature of online interactions, such as email or social media, may reduce immediacy and emotional influence. These factors complicate applying and evaluating techniques in digital settings, underscoring the need for frameworks that address these online-specific challenges.

Demographic and Cultural Gaps. While this study introduces a framework for evaluating the effectiveness of psychological techniques, it does not fully explore how demographic or cultural factors may mediate their impact. Differences in compliance across various age groups, genders, or cultural backgrounds remain unexplored. Addressing these demographic considerations in future research would enhance the applicability of these findings and allow for more tailored defenses against social engineering across diverse populations.

6.3. Future Research Directions

In addition to the findings presented in this article, there are several directions for future research and practical initiatives to enhance cybersecurity in the face of social engineering threats.

A promising approach is to conduct a real-world face-to-face (F2F) study. This would involve validating and gaining deeper insights into the effectiveness of psychological techniques, as well as using additional techniques which can only be applied in non-online contexts in practical scenarios. Such a study could help bridge the gap between controlled experiments and real-world social engineering attacks, providing valuable insights for security professionals.

Another area of investigation involves in-depth case studies of actual social engineering attacks. Analyzing tactics employed in attacks such as phishing, pretexting, and tailgating can offer a deeper understanding of the underlying psychological principles at play. These case studies can serve

as valuable resources for both researchers and organizations seeking to bolster their security measures.

NLP and Large Language Models (LLMs) offer powerful techniques for dissecting psychological manipulation in phishing emails and other written communication-based attacks. By identifying persuasive language, authority appeals, and commitment or reciprocity tactics, NLP can help organizations detect and respond to social engineering attempts more effectively. AI technology can be utilized to train models based on parameters defined by NLP, in order to utilize psychological techniques in social engineering scenarios as well as identify them. This in turn will be a valuable indicator for the detection of social engineering attacks such as phishing emails.

Behavioral analysis is another promising avenue for future research. Exploring the behavioral changes in social engineering victims during and after attacks can reveal patterns that aid in improved detection and response strategies. Understanding how individuals react to different social engineering tactics can inform the development of more targeted countermeasures. The behavior of the victims may be analyzed from a psychological standpoint as well as by harnessing the power of AI technology.

The final point is that the development and implementation of social engineering countermeasures are essential. Practical steps, such as employee training, advanced email filtering systems, and awareness campaigns, can help mitigate social engineering risks within organizations. These countermeasures play a crucial role in strengthening the human element of cybersecurity.

To summarize, while this article provides valuable insights into the effectiveness of psychological techniques in social engineering, there is still much to explore and implement. By pursuing these avenues of research and practical initiatives, we can better protect individuals and organizations from the ever-evolving landscape of social engineering threats.

7. Conclusion

In this study, we delved into the complex world of psychological techniques utilized in online phishing attacks, exploring how these methods exploit human cognitive biases to manipulate individuals. Through rigorous analysis, the study has introduced and validated novel metrics such as Absolute Compliance Increase Rate (ACR), Relative Compliance Increase Rate (RCR), and Comprehensive Compliance Increase Rate (CCR), providing a nuanced framework for quantifying the influence of psychological tactics on compliance behaviors.

The findings reveal the importance of group dynamics in compliance and the importance of the majority size, especially in scenarios with initially low compliance, suggesting it is a necessary phenomenon to acknowledge when designing preemptive defense mechanisms. Similarly, established principles such as Authority and Commitment & Consistency were confirmed as highly impactful, aligning with their noted prevalence in both theoretical and practical domains of social engineering. These insights not only enhance our understanding, but also guide effective countermeasures.

Moreover, by providing a detailed taxonomy of psychological techniques used in notable phishing attacks, this article enriches the existing body of knowledge, offering a resource for cybersecurity professionals seeking to understand the interplay between psychology and security. By correlating these techniques with empirical data from time-honored cornerstone studies, as well as contemporary studies, it paves the way for future research aimed at fortifying digital security infrastructures against the subtleties of social engineering.

Overall, this research underscores the importance of integrating psychological insights into cybersecurity practices. It offers a foundation for developing more effective training programs and defensive measures that address the human element, which is often the weakest link in security chains. The clear demonstration of the effectiveness of various social engineering techniques provides a practical basis for developing training programs and defensive protocols against the increasingly sophisticated world of cyber threats.

Acknowledgments

This research has been partially funded from the European Union's research and innovation programmes under grant agreements No. 101070214 (TRUSTEE), No. 101119602 (COBALT), No. 101092702 (OASEES), and No. 101120962 (RESCALE). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Health and Digital Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

References

Abdullahi, A.M., Oyibo, K., Orji, R., Kawu, A.A., 2019. The influence of age, gender, and cognitive ability on the susceptibility to persuasive strategies. Information 10, 352. doi:10.3390/info10110352.

Abroshan, H., Devos, J., Poels, G., Laermans, E., 2021. Phishing happens beyond technology: The effects of human behaviors and demographics on each step of a phishing process. IEEE Access 9, 44928–44949. doi:10.1109/ACCESS.2021.3066383.

Aldawood, H., Skinner, G., 2019. Reviewing cyber security social engineering training and awareness programs—pitfalls and ongoing issues. Future internet 11, 73.

Alshaikh, M., 2020. Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers & Security 98, 102003.

AO Labs, 2023. Unpacking (and preventing) the circleci data breach. https://appomni.com/ao-labs/unpacking-preventing-circleci-data-breach/.

Aronson, E., Blaney, N., Stephan, C., Sikes, J., Snapp, M., 1978. The jigsaw classroom. Sage. doi:10.4324/9781003106760-7.

Asch, S.E., 1952. Group forces in the modification and distortion of judgments. Social psychology , 450–501.

Asch, S.E., 1955. Opinions and social pressure. Scientific American 193, 31–35. URL: 10.1038/scientificamerican1155-31.

Asch, S.E., 1956. Studies of independence and conformity: I. a minority of one against a unanimous majority. Psychological monographs: General and applied 70, 1. doi:10.1037/h0093718.

Asch, S.E., 2016. Effects of group pressure upon the modification and distortion of judgments, in: Organizational influence processes. Routledge, pp. 295–303.

Bargh, J.A., Morsella, E., 2008. The unconscious mind. Perspectives on psychological science 3, 73–79. doi:10.1111/j.1745-6916.2008.00064.x.

BBC News, 2018. British airways breach: How did hackers get in? https://www.bbc.com/news/technology-45446529.

BBC News, 2019. British airways faces record £183m fine for data breach. https://www.bbc.com/news/business-48905907.

BBC News, 2020a. British airways fined £20m over data breach. https://www.bbc.com/news/technology-54568784.

BBC News, 2020b. Major us twitter accounts hacked in bitcoin scam. https://www.bbc.com/news/technology-53425822.

Bem, D.J., 1972. Self-perception theory, in: Advances in experimental social psychology. Elsevier. volume 6, pp. 1–62. doi:10.1016/S0065-2601(08/60024-6.

Bond, R., Smith, P.B., 1996. Culture and conformity: A meta-analysis of studies using asch's (1952b, 1956) line judgment task. Psychological Bulletin 119, 111–137. doi:10.1037/0033-2909.119.1.111.

Bullée, J.W.H., Montoya, L., Pieters, W., Junger, M., Hartel, P., 2018. On the anatomy of social engineering attacks—a literature-based dissection of successful attacks. Journal of investigative psychology and offender profiling 15, 20–45. doi:10.1002/jip.1482.

Burger, J.M., 1986. Increasing compliance by improving the deal: The that's-not-all technique. Journal of Personality and Social Psychology 51, 277–283. doi:10.1037/0022-3514.51.2.277.

Chartrand, T.L., Bargh, J.A., 1999. The chameleon effect: The perception–behavior link and social interaction. Journal of Personality and Social Psychology 76, 893–910. doi:10.1037/0022-3514.76.6.893.

Cialdini, R.B., 1984. Influence: The psychology of persuasion. volume 55. Harper Collins New York.

Cialdini, R.B., 2007. Influence: The psychology of persuasion. volume 55. Collins New York.

Cialdini, R.B., Cacioppo, J.T., Bassett, R., Miller, J.A., 1978. Low-ball procedure for producing compliance: commitment then cost. Journal of Personality and Social Psychology 36, 463. doi:10.1037/0022-3514.36.5.463.

Cialdini, R.B., Vincent, J.E., Lewis, S.K., Catalan, J., Wheeler, D., Darby, B.L., 1975. Reciprocal concessions procedure for inducing compliance: The door-in-the-face technique. Journal of Personality and Social Psychology 31, 206–215. doi:10.1037/h0076284.

Cohen, J., 2016. A power primer.. American Psychological Association. chapter 18. p. 279–284. doi:10.1037/14805-018.

Cooper, H.M., 1979. Statistically combining independent studies: A meta-analysis of sex differences in conformity research. Journal of Personality and Social Psychology 37, 131–146. doi:10.1037/0022-3514.37.1.131.

Daly, A., 2021. 7 of the biggest phishing scams of all time. URL: https://www.inky.com/en/blog/7-of-the-biggest-phishing-scams-of-all-time-2021.

Department of Justice, 2019. Lithuanian man sentenced to 5 years in prison for theft of over $120 million in fraudulent business email compromise scheme. URL: https://www.justice.gov/usao-sdny/pr/lithuanian-man-sentenced-5-years-prison-theft-over-120-million-fraudulent-business.

Dijksterhuis, A., Smith, P.K., van Baaren, R.B., Wigboldus, D.H., 2005. The unconscious consumer: Effects of environment on consumer behavior. Journal of Consumer Psychology 15, 193–202. doi:10.1207/s15327663jcp1503_3.

DocuSign, 2017. Update: 5/15/2017: Latest update on malicious email campaign. https://www.docusign.com/trust/alerts/update-5-15-2017-latest-update-on-malicious-email-campaign.

Eagly, A.H., 1978. Sex differences in influenceability. Psychological Bulletin 85, 86–116. doi:10.1037/0033-2909.85.1.86.

Eagly, A.H., Wood, W., Fishbaugh, L., 1981. Sex differences in conformity: Surveillance by the group as a determinant of male nonconformity. Journal of Personality and Social Psychology 40, 384–394. doi:10.1037/0022-3514.40.2.384.

Enrici, I., Ancilli, M., Lioy, A., 2010. A psychological approach to information technology security, in: 3rd international conference on human system interaction, IEEE. pp. 459–466. doi:10.1109/HSI.2010.5514528.

Ferguson, C.J., 2016. An effect size primer: A guide for clinicians and researchers.. American Psychological Association. chapter 20. p. 301–310. doi:10.1037/14805-020.

Ferreira, A., Teles, S., 2019. Persuasion: How phishing emails can influence users and bypass security measures. International Journal of Human-Computer Studies 125, 19–31. doi:10.1016/j.ijhcs.2018.12.004.

Flores, W.R., Ekstedt, M., 2016. Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. Computers & security 59, 26–44.

Freedman, J.L., Fraser, S.C., 1966. Compliance without pressure: The foot-in-the-door technique. Journal of Personality and Social Psychology 4, 195–202. doi:10.1037/h0023552.

Gragg, D., 2003. A multi-level defense against social engineering. SANS Reading Room 13, 1–21.

Green, B.L., Kenrick, D.T., 1994. The attractiveness of gender-typed traits at different relationship levels: Androgynous characteristics may be desirable after all. Personality and Social Psychology Bulletin 20, 244–253. doi:10.1177/0146167294203002.

Griskevicius, V., Goldstein, N.J., Mortensen, C.R., Cialdini, R.B., Kenrick, D.T., 2006. Going along versus going alone: when fundamental motives facilitate strategic (non) conformity. Journal of Personality and Social Psychology 91, 281. doi:10.1037/0022-3514.91.2.281.

Hertzog, R.L., Scudder, J.N., 1996. Influence of persuader gender versus gender of target on the selection of compliance-gaining strategies. Howard Journal of Communications 7, 29–34. doi:10.1080/10646179609361711.

Jackson, L.A., 1983. The perception of androgyny and physical attractiveness. Personality and Social Psychology Bulletin 9, 405–413. doi:10.1177/0146167283093011.

Jhangiani, R., Tarry, H., 2022. Principles of Social Psychology-1st International H5P Edition. BCcampus.

Kahneman, D., 2011. Thinking, fast and slow. Macmillan.

Kelman, H.C., 1958. Compliance, identification, and internalization three processes of attitude change. Journal of conflict resolution 2, 51–60. doi:10.1177/002200275800200106.

Kiesel, A., Wagener, A., Kunde, W., Hoffmann, J., Fallgatter, A.J., Stöcker, C., 2006. Unconscious manipulation of free choice in humans. Consciousness and Cognition 15, 397–408. URL: 10.1016/j.concog.2005.10.002.

Krebs, B., 2017. Breach at docusign led to targeted email malware campaign. https://krebsonsecurity.com/2017/05/breach-at-docusign-led-to-targeted-email-malware-campaign/comment-page-1/.

Krombholz, K., Hobel, H., Huber, M., Weippl, E., 2015. Advanced social engineering attacks. Journal of Information Security and Applications 22, 113–122. doi:10.1016/j.jisa.2014.09.005.

Lakin, J.L., Jefferis, V.E., Cheng, C.M., Chartrand, T.L., 2003. The chameleon effect as social glue: Evidence for the evolutionary significance of nonconscious mimicry. Journal of nonverbal behavior 27, 145–162. URL: 10.1023/A:1025389814290.

Langer, E.J., Blank, A., Chanowitz, B., 1978. The mindlessness of ostensibly thoughtful action: The role of" placebic" information in interpersonal interaction. Journal of Personality and Social Psychology 36, 635. doi:10.1037/0022-3514.36.6.635.

Lichumon, 2023. 5 worst whaling attacks: Whale phishing. PhishGrid. URL: https://phishgrid.com/blog/worst-whaling-attack/}1-snapchat-payroll-information-leak.

Major, B., Deaux, K., 1977. Effects of physical attractiveness, sex and sex-role on trait attributions. Midwestern Psychological Association Convention .

Mann, L., 1969. Social Psychology. volume 55. Wiley.

Milgram, S., 1974. Obedience to Authority: An Experimental View. Harper & Row, New York.

Milgram, S., Bickman, L., Berkowitz, L., 1969. Note on the drawing power of crowds of different size. Journal of Personality and Social Psychology 13, 79–82.

Mitnick, K.D., Simon, W.L., 2003. The art of deception: Controlling the human element of security. John Wiley & Sons.

Mitnick Security, 2020. The 2020 twitter bitcoin scam: How it happened and key lessons from whitehat hacker kevin mitnick. https://www.mitnicksecurity.com/blog/2020-twitter-bitcoin-scam.

Montañez, R., Golob, E., Xu, S., 2020. Human cognition through the lens of social engineering cyberattacks. Frontiers in psychology 11, 1755. doi:10.3389/fpsyg.2020.01755.

Morrison, C., Naumov, P., 2019. Group conformity in social networks. Journal of Logic, Language and Information 29, 3–19. doi:10.1007/s10849-019-09303-5.

Muscanell, N.L., Guadagno, R.E., Murphy, S., 2014. Weapons of influence misused: A social influence analysis of why people fall prey to internet scams. Social and Personality Psychology Compass 8, 388–396. doi:10.1111/spc3.12115.

New York Department of Financial Services, 2020. Twitter investigation report. https://www.dfs.ny.gov/Twitter_Report.

Newell, B.R., Shanks, D.R., 2014. Unconscious influences on decision making: A critical review. Behavioral and Brain Sciences 37, 1–19. doi:10.1017/s0140525x12003214.

Nowak, K.L., Rauh, C., 2017. The Influence of the Avatar on Online Perceptions of Anthropomorphism, Androgyny, Credibility, Homophily, and Attraction. Journal of Computer-Mediated Communication 11, 153–178. doi:10.1111/j.1083-6101.2006.tb00308.x.

Nwankpa, J.K., Datta, P.M., 2023. Remote vigilance: The roles of cyber awareness and cybersecurity policies among remote workers. Computers & Security 130, 103266.

Oinas-Kukkonen, H., Harjumaa, M., 2009. Persuasive systems design: Key issues, process model, and system features. Communications of the Association for Information Systems 24, 28. doi:10.17705/1CAIS.02428.

Perception Point, 2023. Takeaways from the circleci incident. https://perception-point.io/blog/takeaways-from-the-circleci-incident/.

Purohit, A., 2022. 5 of the most expensive phishing scams in history. URL: https://www.delta-net.com/blog/5-of-the-most-expensive-phishing-scams-in-history/.

Saul, M., 2023a. The milgram shock experiment. www.simplypsychology.org/milgram.html.

Saul, M., 2023b. What is conformity? www.simplypsychology.org/conformity.html.

Sawyer, B.D., Hancock, P.A., 2018. Hacking the human: The prevalence paradox in cybersecurity. Human factors 60, 597–609. doi:10.1177/0018720818780472.

Schneier, B., 2015. Secrets & Lies: digital security in a networked world. Wiley. doi:10.1002/9781119183631.

Sherif, M., 1988. The robbers cave experiment: Intergroup conflict and cooperation.[Orig. pub. as Intergroup conflict and group relations]. Wesleyan University Press.

Sigalos, M., 2022. Crypto hackers steal over $615 million from network that runs popular game axie infinity. https://www.cnbc.com/2022/03/29/hackers-steal-over-615-million-from-network-running-axie-infinity.html.

Source Defense, 2022. British airways: A case study in gdpr compliance failure. https://sourcedefense.com/resources/blog/british-airways-a-case-study-in-gdpr-compliance-failure/.

Stallen, M., Smidts, A., Sanfey, A., 2013. Peer influence: neural mechanisms underlying in-group conformity. Frontiers in Human Neuroscience 7. URL: https://www.frontiersin.org/articles/10.3389/fnhum.2013.00050, doi:10.3389/fnhum.2013.00050.

Steele, R.S., Morawski, J.G., 2002. Implicit cognition and the social unconscious. Theory & Psychology 12, 37–54. doi:10.1177/0959354302121003.

Stojnic, T., Vatsalan, D., Arachchilage, N.A.G., 2021. Phishing email strategies: Understanding cybercriminals' strategies of crafting phishing emails. SECURITY AND PRIVACY 4. doi:10.1002/spy2.165.

Stylianou, I., 2021. Analysis and usage of penetration testing tools.

Tessian, 2023. 15 examples of real social engineering attacks. URL: https://www.tessian.com/blog/examples-of-social-engineering-attacks/.

Tidy, J., 2022. Ronin network: What a $600m hack says about the state of crypto. https://www.bbc.com/news/technology-60933174.

Toulas, B., 2022a. Hackers stole $620 million from axie infinity via fake job interviews. https://www.bleepingcomputer.com/news/security/hackers-stole-620-million-from-axie-infinity-via-fake-job-interviews/.

Toulas, B., 2022b. Office 365 phishing attack impersonates the us department of labor. URL: https://www.bleepingcomputer.com/news/security/office-365-phishing-attack-impersonates-the-us-department-of-labor/.

TrendMicro, 2016. Austrian aeronautics company loses over €42 million to bec scam. URL: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/austrian-aeronautics-company-loses-42m-to-bec-scam.

U.S. Department of Labor, . Guidance on the protection of personally identifiable information (pii). URL: https://www.dol.gov/general/ppii.

Votiro, 2022. Everything we know about the axie infinity breach. https://votiro.com/blog/everything-we-know-about-the-axie-infinity-breach/.