Does Security Attitude Really Predict Susceptibility to Persuasion Tactics in Social Engineering Attempts?

Aya Muhanad[1] [0009-0009-0708-4183], Tourjana Islam Supti[1] [0000-0002-1302-1607], Israa Abuelezz[1][0000-0002-1082-6864], Ala Yankouskaya[2] [0000-0003-0794-0989], Khaled Khan[1] [0000-0002-8848-0760], Mahmoud Barhamgi[1] [0000-0003-2974-3951], Armstrong Nhlabatsi[1] [0000-0002-3407-7466]1, Raian Ali[3] [0000-0002-5285-7829]

[1]College of Engineering, Qatar University, Doha, Qatar

[2]Department of Psychology, Bournemouth University, Poole, UK

[3]College of Science and Engineering, Hamad Bin Khalifa University, Doha, Qatar

Abstract

Purpose – This study investigates whether an individual's security attitude (SA) predicts susceptibility to persuasion in social engineering (SE) attempts.

Design/methodology/approach – We examined susceptibility to Cialdini's six principles of persuasion in SE contexts. 323 participants from the United Kingdom and 329 from Arab Gulf Cooperation Countries (Arab GCC) were surveyed. Participants were presented with 12 scenarios involving a request to download an app from a member of a social media group, six persuasive scenarios and six neutral counterparts. The six-item security attitude scale (SA-6) measured participants' attitudes toward security practices.

Findings –Some positive correlations were found between SA and vulnerability to specific persuasion principles. Regression analyses indicated that SA was a significant predictor of vulnerability. Notably, higher SA was associated with slightly increased vulnerability in all significant models.

Practical Implications – These findings highlight the need for effective strategies to resist SE attacks involving immunity to persuasion tactics. Individuals with higher security attitudes may be overconfident and underestimating risks.

Originality – The effect of persuasion was uniquely distilled and measured by the difference between the impact of the persuasion scenario and its neutral version, representing a method novelty. Furthermore, it includes a sample from the Arab GCC, an often-neglected population in research. The paper is the first to compare SA, related to security knowledge-seeking and following security recommendations, with psychological immunity to persuasion in a security context.

Keywords: Social Engineering, Security Attitude, Persuasion, Cialdini Principles, Risk-Taking, Arab, UK

Paper Type: Research paper

Introduction

Persuasion is a form of human communication with the goal of influencing the choices and perceptions of others (Jones and Simons, 2017). It is used in multiple situations, from parents advising their children (Azizah, 2020), to entities seeking confidential information for malicious purposes (Jones *et al.*, 2021). Persuasion can change an individual's beliefs and behavior (Murphy *et al.*, 2003), making it a potential threat. While many companies use commercial security products for protection, the real losses result from sophisticated social engineering (SE) attacks that obtain access to systems through the deception of a trusted user (Mitnick and Simon, 2002). In SE attacks, human traits are treated as vulnerabilities and are weaponized to persuade, deceive, and manipulate victims (Tsinganos *et al.*, 2018). With the growth of open-source intelligence, gathering information on victims becomes easier, enabling attacks to occur on a much larger scale (Wang *et al.*, 2021). These concerns emphasize the necessity of increasing individuals' resilience against SE attacks that employ persuasion.

Previous research has identified various approaches to distinguish between different persuasion techniques. A notable classification of persuasion tactics was established by Robert Cialdini, who identified six persuasion principles commonly used by people. These principles include social proof, where individuals look to others for guidance in uncertain situations; authority, which refers to the inclination to follow the advice of experts; reciprocity, which creates a sense of obligation to return favors; commitment/consistency, the impact of previous commitments on future decision-making and the desire for consistency; likeability, the tendency to follow or comply with those we like and can relate to; and scarcity, which leverages urgency and limitation to compel certain actions (Cialdini, 2001). These principles have been extensively studied in various fields such as health and marketing (Franke *et al.*, 2009; Gaube *et al.*, 2020), but are also employed in cyberattacks such as SE attempts. Akbar (2014) found that 96.1% of 207 phishing emails analyzed used the principle of authority and 41.1% used scarcity, highlighting the frequent use of Cialdini's principles in SE attempts. Their effectiveness in increasing online risk-taking has also been proven in situations where people were already aware of the risk, raising concerns about their use in SE attacks (Mollazehi *et al.*, 2024).

Social engineering attacks have become increasingly sophisticated and pose a real danger to users. A study conducted a simulation in which unsolicited emails were sent to 150 members of a pharmaceutical company. The results revealed that 85% of the receivers opened the email and downloaded the files (Gallegos-Segovia *et al.*, 2017). These figures are concerning, as a real attack could lead to major consequences. An example of such losses was reported by the New York Times when its employees received fake FedEx notifications containing malware (Perlroth, 2013). As a result, the credentials of both employees and reporters were stolen. Similarly, employees at Twitter experienced SE attacks, resulting in several celebrity accounts being compromised (*BBC News,* 2020). Not only are larger organizations at risk; but average Microsoft users are also targeted (Sharma, 2021). The success of such SE attacks often depends on the persuasion methods used to manipulate victims into carrying out certain actions or revealing sensitive information (Siddiqi *et al.*, 2022).

To enhance individuals’ resistance to persuasion tactics, researchers explore human vulnerabilities to better understand susceptibility. Numerous studies have utilized personality constructs to identify those who are more susceptible to persuasion e.g. (Oyibo and Vassileva, 2019; Wall *et al.*, 2019). However, personality traits alone do not significantly account for susceptibility to persuasion in SE attempts (Muhanad *et al.*, 2024). It is important to consider individuals' attitudes toward security measures and their willingness to follow advice from cybersecurity experts. In addition to assessing their perspective on security measures, researchers must also evaluate their likelihood of successfully applying this advice in real-world situations. Previous research indicates that some individuals perceive themselves as less vulnerable to persuasive messages, such as advertising, compared to others (Douglas *et al.*, 2010). Ironically, people who believed themselves as invulnerable to deception were less likely to resist the deception (Sagarin *et al.*, 2002). This raises an important question about how an individual's intent to implement security measures aligns with their behaviour, and whether they can effectively resist persuasion in SE attacks.

Understanding an individual's attitudes can provide more insights into intentions and behaviours. Attitude can be defined as an individual’s inclination to respond either positively or negatively to something or someone based on the individual’s evaluation (Vargas-Sánchez *et al.*, 2016). In the context of security, an individual’s attitude can aid us in understanding the intentions and the likelihood of implementing security behaviours (Faklaris *et al.*, 2019). To enhance individuals' resistance to persuasion, it is essential to discern whether they intend to adhere to security protocols. A study examining the attitudes of small and medium-sized enterprises towards cybersecurity measures identified several factors contributing to negative sentiments (Wilson *et al.*, 2023). These factors include challenges in staying current with evolving threats, misconceptions about their own vulnerability to attacks, and feelings of being overwhelmed by cybersecurity requirements, all of which can lead to a disconnection from security practices. Other researchers have also linked behaviour, feelings, and knowledge with attitude, assuming that one's understanding of security and personal sentiments can influence security behaviour (Szűcs *et al.*, 2024).

Organizations are implementing security awareness programs to turn humans from the vulnerability to the strongest link in the security chain (Assenza *et al.*, 2020). However, a major problem is the lack of measurement of the effectiveness of such security awareness programs (Assenza *et al.*, 2020). This raises the question of whether security awareness genuinely enhances resistance to SE attacks. A notable limitation observed in several studies lies in the reliance on security intentions or self-reported measures, rather than combining these with behavioural measures, such as determining whether individuals can be tricked into clicking unknown links (Bayl-Smith *et al.*, 2022). Through this study, we aim to investigate whether an individual's attitude towards security measures can explain susceptibility to online persuasion that encourages risky online behaviour.

Several studies have shown that users who evaluated themselves or proved to have security knowledge, usually intend to use and practice cybersecurity measures. A study that assessed user knowledge of phishing attacks through direct and indirect survey questions revealed that users' knowledge positively correlated with the intention and adoption to use anti-phishing practices (Wang, 2013). Another survey confirmed these findings, showing that participants with knowledge of phishing attacks were better protected against such attacks (Downs *et al.*, 2007). However, the aforementioned studies focused on phishing attacks, which are only one type of SE attack, and did not distil the susceptibility to persuasive elements in the messages that encourage risky online behaviour. In our study, we want to investigate the relationship between security attitude (SA) and susceptibility to persuasion in potential SE attempts, especially in scenarios where users are already aware of potential risks.

Exploring how SA affects susceptibility to persuasion tactics across various cultures reveals nuanced interactions between these strategies and specific cultural contexts. Research indicates that cultural background does not necessarily affect vulnerability to Cialdini's six persuasion principles (Muhanad *et al.*, 2024), but culture was shown to affect privacy attitude (Halevi *et al.*, 2016). Although privacy attitude differs slightly from SA in the sense that it focuses on the attitude towards sharing information online, it can indicate that possible cultural differences exist for SA as well. Furthermore, studies have shown that Western cultures tend to be more individualistic (Markus and Kitayama, 1991), while Arab cultures share more collectivistic values (Alnunu *et al.*, 2021). Given these distinctions, examining how SA affects susceptibility to Cialdini's principles between various cultural dimensions within the realms of SE can provide valuable insights. Research on human factors in cybersecurity is largely biased towards the Western world, with the U.S. leading at 60%, followed by Germany, the Netherlands, and Italy, each at 10% (Rohan *et al.*, 2021). This concentration on Western populations risks overlooking the distinctive characteristics of collectivist cultures, such as those in Arab societies, where a preference for uncertainty avoidance ("Hofstede's Globe", 2015) and communal norms can shape decision-making processes.

Although Cialdini's principles have been investigated for their general impact on behaviours, their specific relationship with SA in decision-making, particularly in risk-related online situations where individuals are aware of the risk, has not been extensively studied. In other words, it remains unclear whether SA translates to greater or lesser susceptibility to persuasion when risk is already apparent. This study has the methodological strength of using both persuasion presence and absence counterparts' scenarios, allowing for a more accurate distillment of the effect of Cialdini's principles on susceptibility to SE attempts. Additionally, it includes an often-underrepresented cultural group, the Arab sample, addressing a gap in previous research. Based on these foundations, our study decided to answer the following research question:

RQ1: *Can security attitude predict the degree to which individuals resist persuasion in social engineering attempts?*

The rest of the manuscript is structured as follows: Section 2 explains the method of this study, Section 3 presents the results, and Sections 4, 5, and 6 provide the discussion, implications, and limitations respectively. The last section concludes the findings of this paper.

Method

This section focuses on how we collected our data and recruited participants. It also explains the design of our study and details the face validation process. Lastly, it describes the statistical approach used.

Participants Recruitment & Dataset

The participants were selected from two regions: the Arab Gulf Cooperation Council (GCC) and the United Kingdom (UK) with the assistance of TGM Research (https://tgmresearch.com/), a company that specializes in data collection from target audiences. Both regions offer diverse populations due to their different cultures and norms, reflected in the Power Distance and Individualism country comparison charts (“Hofstede’s Globe”, 2015). The surveys were created using SurveyMonkey (www.surveymonkey.com), an online survey design tool. The survey consisted of scenarios on Cialdini’s principles and questions related to security attitudes. Participants had to meet eligibility criteria, including being aged 18 or above and having been born in a GCC country (Kingdom of Saudi Arabia, Kuwait, Oman, Bahrain, United Arab Emirates, or Qatar) or the UK (Ireland, Scotland, England, or Wales), and self-identify as Arabs or British in terms of norms and culture. To ensure data accuracy, attention checks were integrated into the survey questions, and failure to pass these checks disqualified the participant. Furthermore, completing the survey in less than 50% of the median duration resulted in disqualification. The median was calculated after removing durations that were twice the expected time or more, primarily due to assuming inactivity during certain periods of survey completion. All participants provided their informed consent and were allowed to stop participation at any point. Ethical approval for this study was obtained from the Institutional Review Board at the last author’s institution. We could not get Arab participants above 60 which caused uneven distribution in terms of age groups amongst the two studied populations. This age group was excluded from the dataset. The final dataset included 652 participants, with 329 participants from the Arab GCC and 323 from the UK.

Study Design

The survey consisted of scenarios related to Cialdini's principles and measurement items that assess the security attitudes of participants. The survey displayed a series of 12 scenarios to evaluate the influence of each of Cialdini's six principles of persuasion. The scenarios refer to a social media group where a member, who is a software designer, asked for volunteers to install a new app to provide feedback. The mobile app collects personal data such as age, interests, and financial status to provide unique and customized recommendations to the user. The eligibility criteria included regular social media use and a general openness to helping strangers. For each persuasion principle, a scenario was created where the principle was employed to encourage participants to install the app and one counterpart scenario where it was neutralized. Since there are six persuasion principles, a total of 12 scenarios were designed, which were randomized by SurveyMonkey to reduce order effects. The scenarios were carefully constructed to solely represent the specific persuasion principle they focused on. To eliminate potential cultural biases, the member was presented as 'Majid' for Arab GCC participants and 'Oliver' for UK participants. These names were selected to ensure they do not carry any religious connotations

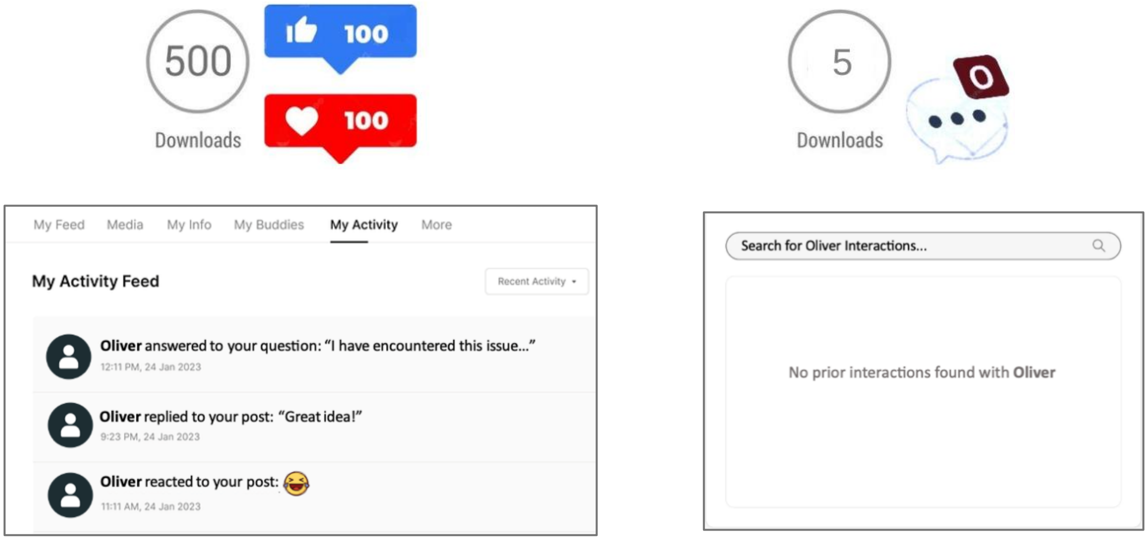
The app in the presented scenarios collects personal data such as age, name, location, dietary preferences, and activity details to provide a customized user experience, which includes health plans and dining options. Accepting to install and provide the data should raise concerns about privacy and security among participants. Participants were questioned whether they were aware of the potential risks of installing such an app. Those who did not see any risks in that were excluded from the study as our purpose is to test the effect of persuasion knowledge where risk is already recognized. Figure 1 illustrates the scenarios related to social proof and reciprocity for participants in the UK. The presence of social proof was portrayed by showing that the app had many likes and downloads, while the absence scenario was represented by showing zero comments and five downloads. As for the reciprocity principle, the participant had to imagine that they had previously communicated with Oliver (i.e. the software designer/potential social engineer). In the presence scenario, Oliver liked and responded to the participant's posts, and helped the participant in the past, potentially causing the participant to feel obliged to install the app. Conversely, the absence of reciprocity was illustrated by having no previous interactions with Oliver. In addition to the visual representation, the participants were provided short descriptions to aid them in understanding the scenarios. The presence and absence scenarios for the remaining principles can be accessed through the Open Science Framework (OSF) link in the supplementary materials section.

Face Validation

After we designed the 12 scenarios, we conducted a test to ensure that the scenarios correctly represented the principles and would be clear to participants. We conducted a face validation with three participants from the Arab region and three from European countries. These six individuals were made familiar with Cialdini’s principles. For each scenario, we asked them which principles were represented in the scenarios. The same process was done for the scenarios where the persuasion principles were absent. We refined the scenarios to ensure that each presence scenario represents one and only one of the principles, while the corresponding absence scenario eliminates it. This was done without making the absence scenario discouraging, but rather neutral. In addition to evaluating the scenarios, we asked the individuals whether the avatar of Oliver/Majid showed any religious, financial, or character indicators. This was done to ensure that the avatar did not signal traits or demographics which can influence the effect of the persuasion principles. The six participants were also invited to share observations which helped us improve the scenarios. For example, we readjusted the scenario representing the absence of social proof. Initially, this scenario showed zero downloads, however, this might have caused participants to view this scenario negatively. Therefore, we decided to change it from zero to five downloads.

Measures

This subsection provides a detailed explanation of the measurement instruments included in our survey. Susceptibility to persuasion and security attitude are measured using quantitative measures. The six-item security attitude (SA-6) scale developed by Faklaris, Dabbish, and Hong, allows researchers to assess and compare attitudes towards the usage and adoption of security practices recommended by experts (Faklaris *et al.*, 2019). Due to its short nature compared to other scales such as the 31-item Personal Data Attitude (Addae *et al.*, 2017) measure for adaptive cybersecurity, it can be used in surveys with short measurement time. The items of the scale are found in Table I, to which participants responded using a range from "Strongly Disagree (1)" to "Strongly Agree (5)". The corresponding Arabic version is presented in Table II. The items were translated to Arabic using a back translation process (Brislin, 1970), which involves translating the Arabic text back into English and comparing it to the source text. Participants’ SA_Total scores were calculated by summing scores of the six SA items, providing an overall measure of attitude for consistent comparisons among participants. The scale SA-6 demonstrated good reliability in both samples, with Cronbach’s alpha values of 0.87 for the UK sample and 0.79 for the Arab sample.



My Activity Feed

Oliver answered to your question: “I have encountered this issue...”
12:11 PM, 24 Jan 2023

Oliver replied to your post: “Great idea!”
9:23 PM, 24 Jan 2023

Oliver reacted to your post: 😂
11:11 AM, 24 Jan 2023

No prior interactions found with **Oliver**

Figure 1: Presence (left) and absence (right) of reciprocity (bottom) and social proof (top)

To be recruited, participants needed to see at least minimal risk in installing and testing the app and be aware of the potential security implications. Our purpose was specifically to examine the influence of Cialdini's persuasion principles when there is awareness of the associated risks. We confirmed this by including a question to ensure the participants' awareness of potential risks. To measure susceptibility to persuasion, each scenario was accompanied by two questions. The first question, "In a similar scenario, how likely are you to install the app and give it a try?" Participants were asked to respond on a scale from "Very unlikely (1)" to "Very likely (6)." The second question, "In a similar scenario, how much do you trust Oliver’s (Majid’s for Arab) transparency and intentions?" The response options for this question ranged from "Complete distrust (1)" to "Complete trust (6)." Both questions were included in all scenarios, regardless of whether the principle was present or absent, enabling us to measure the impact of each principle effectively. We calculated two new variables, one known as *Delta Install*, which represents the effect of the principle on the likelihood of installing the app (risk-taking) and another is *Delta Trust,* which represents the effect of the principle on the degree of trust in the software designer (Oliver/Majid). The *Delta* was calculated by subtracting the score when the persuasion was absent from the score when the persuasion was present. The *Delta* ranges from -5 to 5; the higher the *Delta* score, the more susceptible the participant is to the persuasion principle. We consider this a methodological strength, as it allows us to measure the influence of the principle itself and isolate the effects of other factors that might be present in the scenarios.

Table I. The items of Security Attitude (SA-6) scale (Faklaris *et al.*, 2019)

Code	Scale Items
SA_1	I seek out opportunities to learn about security measures that are relevant to me
SA_2	I am extremely motivated to take all the steps needed to keep my online data and accounts safe
SA_3	Generally, I diligently follow a routine about security practices
SA_4	I often am interested in articles about security threats
SA_5	I always pay attention to experts' advice about the steps I need to take to keep my online data and accounts safe
SA_6	I am extremely knowledgeable about all the steps needed to keep my online data and accounts safe

Table II. Our Arabic translation of the SA-6 scale

Scale Items	Code
أبحث دائمًا عن الفُرُص للتعلم حول تدابير الأمان التي تكون ذات صلة بي.	SA_1
أنا مُتحفّز للغاية لاتّخاذ جميع الخطوات الضرورية للحفاظ على بياناتي وحساباتي على الإنترنت بأمان.	SA_2
عمومًا، ألتزم بشكل دقيق بالروتينيات المتعلقة ممارسات الأمان.	SA_3
غالبًا ما أهتم بقراءة المقالات حول التهديدات الأمني.	SA_4
دائمًا ما أصغي إلى نصائح الخبراء حول الخطوات التي يجب علي اتخاذها للحفاظ على بياناتي وحساباتي عبر الإنترنت بأمان.	SA_5
أنا مضّطلع بشكل كبير بجميع الخطوات الضرورية للحفاظ على بياناتي وحساباتي عبر الإنترنت بأمان.	SA_6

Data Analysis

After collection, the dataset was cleaned and correctly coded using Microsoft Excel to be used in the statistical software JASP version 0.19.1 (https://jasp-stats.org/). We removed participants who failed attention checks or did not observe at least minimal risks in installing the app in the depicted scenario. To answer our research question, we conducted correlation and regression analyses. Since a correlation analysis is usually conducted before regression analysis (Pal and Bharati, 2019), we first conducted a Pearson's correlation to find any relationship between the SA of the participant and the susceptibility to the six persuasion principles. Variables that significantly correlated with the SA_Total score were further analysed using regression analysis. This allowed us to assess how much of the susceptibility to persuasion could be attributed to the SA of the participants.

Results

In this section, we present the results of our analysis, including the correlation and regression analyses for the Arab and UK sample.

Descriptive Statistics

The descriptive statistics of demographic characteristics are presented in

Table III. The gender distribution shows differences between the samples, with a higher percentage of males among Arab participants (56.23%) compared to the British participants (41.80%). As for the age of participants, the mean age for Arab participants (35.67) is slightly lower than that for the British participants (38.41). In both the Arab and UK samples, more participants received a higher education compared to basic education, (81.46%) and (68.42%) respectively. Similarly for employment, most participants in both samples were employed. The mean score for SA_Total among Arab participants (24.46) was higher compared to the UK participants (21.25).

Table III. Participants' demographics

Variables	***Participants (N = 652)***	
	Arab (N = 329)	*UK (N = 323)*
Gender (%)		
Male	185 (56.23%)	135 (41.80%)
Female	144 (43.77%)	188(58.20%)
Age		
M (SD)	35.67 (10.15)	38.41 (12.53)
Range	18-60	18-60
Education (%)		
Basic Education	61 (18.54%)	102 (31.58%)
Higher Education	268 (81.46%)	221 (68.42%)
Employment (%)		
Student	14 (4.26%)	19 (5.88%)
Employed/Self-Employed	262 (79.64%)	236 (73.07%)
Unemployed	53 (16.12%)	68 (21.05%)
Security Attitude Total		
M (SD)	24.46 (3.17)	21.25 (4.45)

Results of the UK Sample

We first conducted a correlation analysis to identify any significant relationships. The significant correlations were further evaluated with regressions.

Correlation Analysis: Relationship Between Security Attitude Total, Install (Risk-Taking), and Trust

A sample size of at least 50 is recommended (Fraenkel *et al.*, 2012) to conduct a correlation analysis between variables. Since our data is far beyond that we conducted a correlation between the SA_Total score and the effect (i.e. the delta score) of each persuasion principle on the likelihood of installing the app (Install) and the degree of trust in the software designer (Trust). The delta represents the difference between the scenario where the principle was present and the scenario where the corresponding principle was absent. The same analysis for the presence and absence score separately can be found in Appendix A on the OSF link.

The normality of variables was further confirmed for all variables with skewness and kurtosis in the range ±2 (George and Mallery, 2010). However, the variables for Commitment/Consistency_Install, Commitment/Consistency_Trust, and Scarcity_Trust did not meet this range, therefore a boxplot analysis was conducted for these variables. The Tukey method {25th Quantile - [1.5 x (75th Quantile – 25th Quantile)]} and {75th Quantile + [1.5 x (75th Quantile – 25th Quantile)]} identified 18 outliers for Commitment/Consistency_Install, 10 outliers for Commitment/Consistency_Trust and 10 outliers for Scarcity_Trust, which we updated to either represent the minimum or maximum of the sample without outliers. Updating these outliers did not affect the significance of the correlations, except for the correlation between Scarcity_Trust and the SA_Total score; with the outliers, the correlation was significant, but when updated, the correlation was no longer significant.

We used Pearson's correlation despite our ordinal data since other researchers have proven that the parametric test (i.e. Pearson's correlation) is insensitive to the type of scale used (Havlicek and Peterson, 1976). We explored the relationship between SA_Total and the likelihood of installing the app (risk-taking). The results (see Table IV) show nonsignificant correlations between the SA_Total score and Social Proof, Authority, Commitment/Consistency, and Scarcity. The principle of Likeability (r = 0.17, p = .003) and Reciprocity (r = 0.12, p = .03) had positive significant correlations with the SA_Total score. Indicating that a higher likelihood of installing the app due to these principles correlated with a higher SA.

We further explored the relationship between the SA of an individual and the degree of trust in the intentions of the potential social engineer when persuasion was applied. A Pearson correlation analysis (see Table IV) was conducted and showed no significant correlations between the SA_Total score and the principles of Social Proof, Authority, Commitment/Consistency, Reciprocity, and Scarcity. Only Likeability (r = 0.16, p = .01) had a significant correlation with SA_Total, meaning that a higher degree of trust in the software designer due to the Likeability principle correlated with higher SA. A similar correlation for each scale item individually with the persuasion principles can be found in Appendix B on the OSF link.

Table IV. Pearson's Correlations of Security Attitude Total with Install and Trust for each Persuasion Principle in the UK sample.

Principle	**Install**	**Trust**
Social Proof	-0.01	0.11
Likeability	0.17***	0.16**
Authority	0.09	0.05
Commitment Consistency	-0.01	-0.01
Reciprocity	0.12*	0.11
Scarcity	0.07	0.09

**p < 0.05, **p < 0.01, ***p < 0.001*

Linear Regression Analysis: Security Attitude Total as a Predictor for Install (Risk-Taking) and Trust

After examining the correlation between the variables, we further analyzed the significant correlations using linear regression (Table V). We conducted a linear regression analysis for Likeability_Install, Reciprocity_Install, and Likeability_Trust variables. The regression analyses for the presence and absence variables individually can be found in Appendix C on the OSF link. Using case-wise diagnostics for the linear regression, we removed outliers with a standardized residual exceeding ±3 standard deviation. We removed records for Likeability_Install (n = 2), Reciprocity_Install (n =1), and Likeability_Trust (n = 1). The normality of standardized residuals was assessed using the normal Q-Q plots, where the records were approximately aligned along the diagonal line. Homoscedasticity was confirmed using residuals vs predicted values plots, where the dots did not form any megaphone shapes around the zero line. The Durbin-Watson values for all regression models did not exceed 2.15, which is below 2.5, indicating the absence of autocorrelation between the residuals.

Linear regression analyses were conducted to determine if SA_Total could predict risk-taking and trust due to certain persuasion principles. The models for Likeability_Install, Reciprocity_Install, and Likeability_Trust were all statistically significant, indicating that SA_Total had an effect, though minimal, on these outcomes. The regression analyses for Likeability_Install and Reciprocity_Install described how well SA can predict risk-taking (i.e. the likelihood of installing the app) due to the principle. As for Likeability_Trust, the model measured whether SA could predict the degree of trust the participant placed in the potential social engineer due to the likeability principle. The results of the significant regressions (see Table V) show that SA_Total was a positive predictor in all cases and explained 2–3% of the variance in each dependent variable. We also checked whether the relationship is U-shaped instead of linear by creating a new ordinal variable for SA with categories: 'low,' 'medium,' and 'high'. We compared the means of each of the delta scores to see whether individuals with low SA exhibited behaviour similar to those with high SA; however, this was not the case.

Table V. Significant Linear Regressions with Security Attitude Total as Predictor for Install and Trust in the UK sample.

Outcome	**Predictor**	***B***	***SE***	***t***	***p***	***R*²**	**Adj. *R*²**	***F***
Likeability_Install	SA_Total	0.05^{**}	0.02	3.28	.001	0.03	0.03	10.73
Reciprocity_Install	SA_Total	0.04^{*}	0.02	2.49	.01	0.02	0.02	6.21
Likeability_Trust	SA_Total	0.05^{**}	0.02	3.14	.002	0.03	0.03	9.87

**p < 0.05, **p < 0.01, ***p < 0.001*

Since the effect size of SA_Total as a predictor for susceptibility to likeability and reciprocity was small, we conducted the same regressions using the Bayesian approach. The results provided strong evidence for the likeability regression models. The Bayesian approach assigns probabilities for the hypotheses, the hypothesis in our case is SA acting as a predictor of susceptibility to persuasion. The complete analysis can be found in Appendix C on the OSF link.

Results of the Arab Sample

We first conducted a Pearson's correlation analysis to identify any significant relationships. The significant correlations were further evaluated with regressions.

Correlation Analysis: Relationship Between Security Attitude Total, Install (Risk-Taking), and Trust

To measure if SA can predict or explain the variance in susceptibility to persuasion, we similarly conducted a Pearson correlation (see Table VI) between the SA _Total score and the effect of each persuasion principle (i.e. the delta) on *Install* and *Trust*. The analysis for the presence and absence variables separately can be found in Appendix A on the OSF link. The skewness and kurtosis values were in the range ±2 (George and Mallery, 2010), except for Commitment/Consistency_Trust which we handled the same way as for the UK sample. A total of 13 records were updated for Commitment/Consistency_Trust.

We measured the relationship between SA_Total and the likelihood of installing the app (risk-taking). The results (see Table VI) show nonsignificant correlations between the SA_Total score and Social Proof, Commitment/Consistency, and Scarcity. The principle of Likeability (r = 0.16, p = 0.004), Reciprocity (r = 0.14, p = .01), and Authority (r = 0.12, p = .04) had positive significant correlations with the SA_Total score.

We further explored whether there is a relationship between the SA of an individual and the trust in the intentions of the potential social engineer when persuasion was applied. A Pearson correlation analysis (see Table VI) was conducted between the SA_Total score and the delta variables for trust. The analysis shows no significant correlations between the SA_Total score and the principles of Social Proof, Commitment/Consistency, Reciprocity, and Scarcity. Except Likeability (r = 0.15, p = .01) and Authority (r = 0.13, p = 0.02) which have a significant correlation with SA_Total. A similar correlation between each item of the scale and susceptibility to persuasion variables can be found in Appendix B on the OSF link.

Table VI. Pearson's Correlations of Security Attitude Total with Install and Trust for each Persuasion Principle in the Arab Sample

Principle	Install	Trust
Social Proof	0.02	0.07
Likeability	0.16^{**}	0.15^{**}
Authority	0.12^{*}	0.13^{*}
Commitment Consistency	-0.01	0.05
Reciprocity	0.14^{*}	0.10
Scarcity	-0.01	-0.02

**p < 0.05, **p < 0.01, ***p < 0.001*

Linear Regression Analysis: Security Attitude Total as a Predictor for Install (Risk-Taking) and Trust

The significant correlations were followed up by a linear regression (see Table VII). Records with standardized residuals that exceeded the standard deviation of ±3 were removed. Records were removed for Likeability_Install (n = 1), Authority_Install (n = 3), Reciprocity_Install (n = 1), and Authority_Trust (n = 1). The normality of standardized residuals was confirmed using Q-Q plots, where the dots are approximately aligned along the diagonal line. Homoscedasticity was confirmed using residuals vs. predicted values plots, where the dots did not form any megaphone shapes around the zero line. All Durbin-Watson values did not exceed 2.05, confirming the absence of autocorrelation between residuals.

We conducted linear regression analyses to examine whether SA_Total predicts susceptibility to persuasion tactics, specifically the principles that revealed significant correlations (see Table VI). The regressions (see Table VII) showed that SA_Total was a positive predictor, explaining 2–3% of the variance in risk-taking and trust outcomes. We also checked whether the relationship is U-shaped in the Arab sample instead of linear by creating a new ordinal SA variable with categories: 'low,' 'medium,' and 'high'. We compared the means of each of the delta variables to see whether individuals with low SA exhibited behaviour similar to those with high SA; however, this was not the case.

Table VII. Significant Linear Regressions with Security Attitude Total as Predictor for Trust and Install in the Arab Sample

Outcome	Predictor	*B*	*SE*	*t*	*p*	R^2	Adj. R^2	*F*
Likeability_Install	SA_Total	0.06^{**}	0.02	2.88	.004	0.03	0.02	8.27
Reciprocity_Install	SA_Total	0.07^{**}	0.03	2.76	.01	0.02	0.02	7.59
Authority_Install	SA_Total	0.06^{*}	0.03	2.37	.02	0.02	0.01	5.55
Likeability_Trust	SA_Total	0.06^{**}	0.02	2.67	.01	0.02	0.02	7.15
Authority_Trust	SA_Total	0.06^{*}	0.02	2.30	.01	0.02	0.02	6.74

$*p < 0.05$, $**p < 0.01$, $***p < 0.001$

Since the effect size of SA_Total as a predictor for susceptibility to likeability, authority, and reciprocity was small, we conducted the same regressions using the Bayesian approach. The results provided medium evidence for the likeability regression models and anecdotal evidence for the remaining models. The Bayesian approach assigns probabilities for the hypotheses, the hypothesis in our case is SA acting as a predictor of susceptibility to persuasion. The complete analysis can be found in Appendix C on the OSF link.

Discussion

Our study aims to assess whether an individual's SA can predict their susceptibility to SE attempts. We expect that individuals with a strong understanding of security measures will be resistant to various types of attacks. As Roberts (2021) suggests, cybersecurity attitude positively correlates with cybersecurity knowledge and negatively correlates with risky cyber behaviour. In an organizational setting, employees with higher cybersecurity attitudes also exhibited more cybersecurity knowledge (Williams-Banta, 2019). To measure an individual's SA, we used the SA-6 scale. This scale evaluates how inclined a person is to follow up-to-date security recommendations, protect personal online data, and remain aware of current threats (Faklaris *et al.*, 2019). Typically, individuals with a strong SA are expected to possess more knowledge in the cybersecurity domain than those with a low SA. A strong security mindset is marked by a proactive curiosity about security, both in cyberspace and in other contexts (Schoenmakers *et al.*, 2023). People with such a mindset tend to question the safety of various situations, even in the absence of immediate danger. Similarly, individuals with high SA, driven by their curiosity about security, are expected to behave cautiously, akin to those with a strong security mindset. Our analysis aims to determine whether SA can predict an individual's vulnerability to persuasion in potential SE attempts.

Our study introduces a novel approach to measuring susceptibility to persuasion by creating the delta variable, which quantifies the difference in the likelihood of risk-taking and trusting the software developer in scenarios where persuasion was present versus scenarios where it was neutralized. This variable distils the distinct effect of the persuasion principle. This method offers a significant advancement over previous studies e.g. (Mahmoud *et al.*, 2017; Zalake *et al.*, 2021) that typically measure the impact of persuasion solely based on the presence of persuasion principles. Additionally, measuring both the likelihood of app installation (risk-taking) and the degree of trust in the software designer enhances the robustness of our findings. Measuring several dependent variables improves the reliability of the overall measurement (Schmidt and Hunter, 1996). By capturing these two critical dimensions, our method offers a more comprehensive view of susceptibility to persuasion, highlighting the interplay between risk-taking behaviour and trust in determining the effectiveness of various persuasion principles.

We studied two cultural segments, namely the UK and Arab GCC. Our correlation analysis revealed several patterns in the UK and Arab samples regarding the likelihood of risk-taking and trusting the software designer due to persuasion. In the context of risk-taking, only the likability and reciprocity principles showed significant positive correlations with SA in the UK sample. In the Arab sample, a similar pattern was observed for risk-taking and trust, with the likability and reciprocity principles again showing significant correlations with SA. Additionally, the authority principle also had a significant positive correlation with risk-taking and trust in the Arab sample. This result suggested that there may be a relationship between SA and susceptibility to the likeability, reciprocity, and possibly authority principle. This may initially seem surprising, as a vital security perspective is typically associated with caution rather than risk-taking (Carpenter, 2021; Schoenmakers *et al.*, 2023).

Initially, we only observed the correlations, which can only measure the degree of relationship between variables (Senthilnathan, 2019). Further linear regressions were conducted to confirm if the increased vulnerability can be explained by the participant's SA. For a single predictor, small effect sizes (R^2) are typically expected, ranging from 0.01 to 0.25 (Wall Emerson, 2023). The results for the UK sample revealed two statistically significant regression models for risk-taking and one for trusting the software designer's transparency. Interestingly, individuals with higher SA showed slightly higher susceptibility to likeability and reciprocity persuasion principles than those with lower SA. It is possible that individuals were more likely to take the risk and trust Oliver/Majid because of their amiable character. This could be attributed to the halo effect, where people make assumptions about a person's overall personality based on just one characteristic (Lee and Liang, 2015). The results for the Arab sample showed a similar pattern and included the authority models, where SA_Total was also a positive predictor in risk-taking and trust contexts. While the Bayesian analysis (see Appendix C on the OSF link) showed less supporting evidence for the authority and reciprocity, it showed stronger support for the Likeability_install regressions across both the Arab and UK samples. This suggests that while SA_Total is linked to susceptibility to several principles, the association with the risk-taking (install) due to the likeability principle appears particularly robust across both groups.

Our results can be supported by behavioural science literature, which suggests that processes such as implicit attitudes can influence behaviours, making individuals susceptible to persuasion unconsciously (Cassino *et al.*, 2017). Implicit attitude refers to an attitude that is activated unconsciously, triggered by the memory of a past experience (Colman, 2009). For instance, implicit biases can affect the quality of care provided to different ethnic patient groups in healthcare, even if the healthcare provider is against discrimination (Cherry, 2023). They can also impact hiring practices, performance evaluations, and promotions in the workplace (Ruhl, 2023). A hiring manager might unknowingly favour candidates with similar backgrounds or characteristics, leading to decisions against the best interests of the company. It is possible, that participants with high security attitudes were unconsciously taking more risks due to such implicit attitudes. They might have unknowingly preferred the software designer in the scenarios where he was likeable (i.e. likeability scenario) or provided help (i.e. reciprocity scenario).

The effect of SA suggests that it might have a weak influence on security behaviour in SE scenarios employing persuasion. Persuasion principles are recognized for their ability to alter behaviour (Smith *et al.*, 2014), which could explain why individuals with high SA may struggle to resist persuasion in potential SE attempts. Their slightly higher vulnerability compared to individuals with low SA can be also explained through theoretical frameworks, such as the Elaboration Likelihood Model (Petty and Cacioppo, 1986), which posits that individuals may engage in different processing routes depending on their motivation and ability to process information. For example, in cyber threats where no persuasion is applied, individuals with high SA engage in thorough analytical processing, namely the central route. When being subjected to persuasive messages in SE attempts, due to distraction, individuals with high SA may not carefully evaluate a message and rely on peripheral cues. A peripheral cue can serve as a simple heuristic when the ability to think is low (Cacioppo *et al.*, 2018).

An individual’s SA is significantly shaped by their intention to remain secure online. However, an intention does not always translate into the actual intended behaviour. According to the Theory of Planned Behaviour, several factors, such as perceived behavioural control and actual behavioural control, influence whether intentions lead to action (Ajzen, 1991). For example, even though a person with a strong SA may believe in their ability to follow secure practices, they may not have the actual control to implement these behaviours effectively. This gap can arise due to limited resources, such as insufficient time to thoroughly analyse a message or inadequate skills to recognize persuasion in SE attacks. Since individuals with strong security attitudes often develop their skills by following expert advice, a more thorough analysis of the recommendations they rely on is needed. It is important to examine what these recommendations may be lacking, as inadequate guidance on the psychological aspects of SE could leave individuals unprepared to handle SE attempts effectively. Grimes (2024) suggests that SE is not a primary focus in many of the resources provided by security experts, which may explain why individuals with higher SA struggle to counter SE attempts using persuasion techniques. Moreover, individuals with high SA may underestimate certain recommendations made by security experts and hence take greater risks than those with low SA. Proving that following security recommendations may depend on multiple dimensions, such as how legitimate, effective, and thorough individuals perceive these recommendations (Toro-Jarrin *et al.*, 2024).

The lack of resistance to persuasion in SE attempts among individuals with higher security attitudes could be attributed to overconfidence. Those with elevated SA may believe they are better equipped to control risks, leading them to underestimate potential threats compared to individuals with lower SA. This aligns with the notion that increased security confidence might lead to wrong and less safe online behaviour (Frank *et al.*, 2023). This phenomenon mirrors findings in other domains, such as health behaviour and financial decision-making, where professionals overestimate their abilities. Research in health behaviour shows that some healthcare professionals consider themselves superior to others, leading to suboptimal protective behaviours like poor hand hygiene (Seidel-Fischer *et al.*, 2024). Similarly, financial professionals were found to be overconfident and high risk-takers in financial domains (Broihanne *et al.*, 2014).

In cybersecurity contexts, a study found that personal internet users who rated themselves as knowledgeable about security terms and software often overestimated their ability to defend against attacks (Furnell *et al.*, 2007). Similarly, our results show that individuals with higher security attitudes were slightly more susceptible to persuasion, possibly due to increased confidence. A report by Kroll found that organizations that highly focus on cybersecurity programs were shown to be less able to quickly and accurately detect a threat than they perceived (*The State of Cyber Defense 2023: Detection and Response Maturity Model*, 2023). Individuals who believe they have extensive knowledge may still make incorrect decisions, as they are not true experts in the field (Forget *et al.*, 2016). This cognitive bias is also referred to as the Dunning-Kruger effect, where individuals with limited knowledge sometimes overestimate their competence (Duignan, 2024). It can also be partially explained by the Risk Compensation Theory, where individuals will adjust their risk-taking based on how secure they feel (Johnson, 2017). Overall, the findings suggest that possessing a strong SA can slightly increase vulnerability to SE attacks that employ persuasion.

Implications

The findings of this study have significant implications for cybersecurity recommendation material, awareness, and training programs. These security measures should go beyond technical training and also focus on building psychological resilience against persuasion tactics. The study highlighted that individuals with strong security attitudes were more vulnerable to SE possibly due to overconfidence. This underscores the importance of learning vigilance and humility in the face of cyber threats, regardless of one's level of security knowledge. Furthermore, the results emphasize the need to incorporate psychological factors into security recommendations and training, especially since many individuals who rely on these resources may not fully understand how social engineers exploit human vulnerabilities. Understanding human vulnerabilities has shown success in various fields, including building resistance to persuasion in online gaming (Cemiloglu *et al.*, 2023). Additionally, simply educating about persuasion in security contexts is not enough; employing different behavioural change strategies, like inoculation was proven to be effective (Alshakhsi *et al.*, n.d.). The study identifies various factors such as the Halo effect and implicit biases that could contribute to susceptibility to persuasion among individuals with high security attitudes.

Limitations and Strengths

This study has a limitation in the use of scenario-based surveys, which reduces ecological validity. To mitigate this, we selected scenarios that mirror real-world social media contexts. The scenarios underwent testing before distribution to guarantee their clear representation of persuasion principles. The app installation scenario was chosen for its understandability and popularity. The choice makes it reasonably plausible that any participant completing the online survey can relate to it. We have also provided graphical representations of user interfaces to help participants immerse themselves in the scenarios and aid recall. Eligibility criteria for participants included being social media users and generally open to helping strangers, ensuring that participants could relate to the scenarios. However, more real-world experimentation should be conducted to cover a broader range of SE attacks, as this study focuses on persuasion in a social media scenario. Another issue is the potential for social desirability bias in answering the SA-6 scale. To address this, we ensured participant anonymity, but there is still a possibility that participants may have answered in ways they believed to be more socially acceptable, potentially influencing the accuracy of findings regarding attitudes toward security. Another limitation is the cultural specificity of the study, which focused on samples from the UK and Arab GCC regions. While we chose these two cultural contexts to provide valuable insights into individualistic and collectivist tendencies, the results may not be generalizable to other cultural groups.

Conclusion

This study explored the relationship between an individual's SA and susceptibility to persuasion in a potential SE attack. Security attitude, as measured by the SA-6 scale, was shown to be a statistically significant positive predictor of susceptibility to certain persuasion principles. This suggests that although individuals with higher SA may have more knowledge of online security, they were still more vulnerable to persuasion techniques used by social engineers. The study highlights that knowledge of security measures does not translate into resistance against SE attacks that employ persuasion. Overconfidence in cybersecurity could make individuals more susceptible to persuasion, pointing to the need for assessment measures to be taken by individuals after learning about security. The findings emphasize that current security recommendations need to broaden their focus and include sections on how persuasion operates in SE attacks, ensuring that individuals can recognize and resist these techniques in real-life scenarios. It should also further cover human vulnerabilities to increase awareness of how one becomes a victim of SE attacks. Future research should explore additional factors that might interact with SA, such as emotional states, physical surroundings, or processing time, to better understand the complex dynamics of susceptibility to persuasion in SE attacks.

Conflict of Interest

The authors report there are no competing interests to declare.

Author Contribution

The study was conceptualized, designed, and supervised by RA, MB, and KK. IA, RA, and AN prepared the study materials, collected, cleaned, and scored the data. The statistical analysis was carried out by AM and extended by TS and validated and revised by AY who also contributed to the methodology. The manuscript, including preparing the theoretical underpinning, was written by AM and parts of the introduction and conclusion sections were extended by TS. AY revised the analysis section. The manuscript was reviewed and revised by RA, MB, KK, IA, AN and AY.

Supplementary Material

The study design, dataset, and appendices referred to in this study are available on the following Open Science Framework link: https://osf.io/abuc7/?view_only=f26678171e0e4335b5548719d32714b6.

Funding

This research was made possible by an NPRP-14-Cluster Grant # NPRP 14C-0916-210015 from the Qatar National Research Fund (a member of Qatar Foundation). The findings herein reflect the work and are solely the responsibility of the authors.

References

Addae, J.H., Brown, M., Xu, S., Towey, D. and Radenkovic, M. (2017), "Measuring attitude towards personal data for adaptive cybersecurity", *Information and Computer Security*, Emerald Group Publishing Limited, Bingley, United Kingdom, Vol. 25 No. 5, pp. 560–579, doi: 10.1108/ICS-11-2016-0085.

Ajzen, I. (1991), "The Theory of Planned Behavior", *Organizational Behavior and Human Decision Processes*, Vol. 50, pp. 179–211, doi: 10.1016/0749-5978(91)90020-T.

Akbar, N. (2014), “Analysing Persuasion Principles in Phishing Emails”, info:eu-repo/semantics/masterThesis, University of Twente, October, available at: https://essay.utwente.nl/66177/ (accessed 17 September 2024).

Alnunu, M., Amin, A. and Abu-Rayya, H.M. (2021), “The Susceptibility to Persuasion Strategies Among Arab Muslims: The Role of Culture and Acculturation”, *Frontiers in Psychology*, Vol. 12, p. 574115, doi: 10.3389/fpsyg.2021.574115.

Alshakhsi, S., Al-Thani, D., Männikkö, N. and Ali, R. (n.d.). “Psychological Inoculation against Problematic Social Media Use amongst Adolescents: An Experimental Study”. (Still under review)

Assenza, G., Chittaro, A., De Maggio, M.C., Mastrapasqua, M. and Setola, R. (2020), “A Review of Methods for Evaluating Security Awareness Initiatives”, *European Journal for Security Research*, Vol. 5 No. 2, pp. 259–287, doi: 10.1007/s41125-019-00052-x.

Azizah, Z. (2020), *Persuasive Communication of Parents to Establishment Social Intelligence for the Children*, doi: 10.2991/assehr.k.200217.042.

Bayl-Smith, P., Taib, R., Yu, K. and Wiggins, M. (2022), “Response to a phishing attack: persuasion and protection motivation in an organizational context”, *Information and Computer Security*, Emerald Group Publishing Limited, Bingley, United Kingdom, Vol. 30 No. 1, pp. 63–78, doi: 10.1108/ICS-02-2021-0021.

BBC News. (2020), “Twitter hack: Staff tricked by phone spear-phishing scam”, 31 July.

Brislin, R.W. (1970), “Back-Translation for Cross-Cultural Research”, *Journal of Cross-Cultural Psychology*, SAGE Publications Inc, Vol. 1 No. 3, pp. 185–216, doi: 10.1177/135910457000100301.

Broihanne, M.H., Merli, M. and Roger, P. (2014), “Overconfidence, risk perception and the risk-taking behavior of finance professionals”, *Finance Research Letters*, Vol. 11 No. 2, pp. 64–73, doi: 10.1016/j.frl.2013.11.002.

Cacioppo, J.T., Cacioppo, S. and Petty, R.E. (2018), “The neuroscience of persuasion: A review with an emphasis on issues and opportunities”, *Social Neuroscience*, Taylor & Francis, United Kingdom, Vol. 13 No. 2, pp. 129–172, doi: 10.1080/17470919.2016.1273851.

Carpenter, P. (2021), “The Importance Of A Strong Security Culture And How To Build One”, *Forbes*, 27 May, available at: https://www.forbes.com/councils/forbesbusinesscouncil/2021/05/27/the-importance-of-a-strong-security-culture-and-how-to-build-one/ (accessed 29 October 2024).

Cassino, D., Lodge, M. and Taber, C.S. (2017), “Implicit Political Attitudes: When, How, Why, With What Effects?”, in Kenski, K. and Jamieson, K.H. (Eds.), *The Oxford Handbook of Political Communication*, Oxford University Press, p. 0, doi: 10.1093/oxfordhb/9780199793471.013.59.

Cemiloglu, D., Gurgun, S., Arden-Close, E., Jiang, N. and Ali, R. (2023), “Explainability as a Psychological Inoculation: Building Resistance to Digital Persuasion in Online Gambling through Explainable Interfaces”, *International Journal of Human–Computer Interaction*, Taylor & Francis, Vol. 0 No. 0, pp. 1–19, doi: 10.1080/10447318.2023.2281744.

Cherry, K. (2023), “Is It Possible to Overcome Implicit Bias?”, *Verywell Mind*, 31 May, available at: https://www.verywellmind.com/implicit-bias-overview-4178401 (accessed 29 October 2024).

Cialdini, R.B. (2001), “The Science of Persuasion”, *Scientific American*, Scientific American, a division of Nature America, Inc., Vol. 284 No. 2, pp. 76–81.

Colman, A.M. (2009), “A Dictionary of Psychology”, Oxford University Press.

Douglas, K.M., Sutton, R.M. and Stathi, S. (2010), “Why I am less persuaded than you: People’s intuitive understanding of the psychology of persuasion”, *Social Influence*, Routledge, Vol. 5 No. 2, pp. 133–148, doi: 10.1080/15534511003597423.

Downs, J.S., Holbrook, M. and Cranor, L.F. (2007), “Behavioral response to phishing risk”, *Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit*, presented at the eCrime ’07: eCrime “07 - Anti-phishing working group 2007 eCrime Researchers” Summit, ACM, Pittsburgh Pennsylvania USA, pp. 37–44, doi: 10.1145/1299015.1299019.

Duignan, B. (2024), “Dunning-Kruger effect”, *Enclopedia Britannica*, 21 October, available at: https://www.britannica.com/science/Dunning-Kruger-effect (accessed 27 October 2024).

Faklaris, C., Dabbish, L. and Hong, J.I. (2019), “A Self-Report Measure of End-User Security Attitudes (SA-6)”, *In Proceedings of the Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, presented at the USENIX Association, Berkeley, CA, USA. Available at: https://www.usenix.org/system/files/soups2019-faklaris.pdf

Forget, A., Pearman, S., Thomas, J., Acquisti, A., Christin, N., Cranor, L.F., Egelman, S., *et al.* (2016), “Do or Do Not, There Is No Try: User Engagement May Not Improve Security Outcomes”, *In Proceedings of the Twelfth USENIX Conference on Usable Privacy and Security (SOUPS ’16)*, presented at the USENIX Association, USA, pp. 97–111.

Fraenkel, J.R., Wallen, N.E. and Hyun, H.H. (2012), *How to Design and Evaluate Research in Education*, 8th ed., McGraw-Hill Humanities/Social Sciences/Languages, New York.

Frank, M., Jaeger, L. and Manuel Ranft, L. (2023), “Using contextual factors to predict information security overconfidence: A machine learning approach”, *Computers & Security*, Vol. 125, p. 103046, doi: 10.1016/j.cose.2022.103046.

Franke, N., Keinz, P. and Steger, C.J. (2009), “Testing the Value of Customization: When Do Customers Really Prefer Products Tailored to Their Preferences?”, *Journal of Marketing*, American Marketing Association, Vol. 73 No. 5, pp. 103–121, doi: 10.1509/jmkg.73.5.103.

Furnell, S.M., Bryant, P. and Phippen, A.D. (2007), “Assessing the security perceptions of personal Internet users”, *Computers & Security*, Vol. 26 No. 5, pp. 410–417, doi: 10.1016/j.cose.2007.03.001.

Gallegos-Segovia, P.L., Bravo-Torres, J.F., Larios-Rosillo, V.M., Vintimilla-Tapia, P.E., Yuquilima-Albarado, I.F. and Jara-Saltos, J.D. (2017), “Social engineering as an attack vector for ransomware”, *2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON)*, presented at the 2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON), pp. 1–6, doi: 10.1109/CHILECON.2017.8229528.

Gaube, S., Fischer, P., Windl, V. and Lermer, E. (2020), “The effect of persuasive messages on hospital visitors’ hand hygiene behavior”, *Health Psychology*, American Psychological Association, Washington, US, Vol. 39 No. 6, pp. 471–481, doi: 10.1037/hea0000854.

George, D. and Mallery, P. (2010), *SPSS for Windows Step by Step: A Simple Guide and Reference, 17.0 Update*, 10th ed., Allyn & Bacon, Boston.

Grimes, R. (2024), “If Social Engineering Accounts For Up to 90% of attacks, Why Is It Ignored, Even by CISA? | LinkedIn”, 12 May, available at: https://www.linkedin.com/pulse/social-engineering-accounts-up-90-attacks-why-ignored-roger-grimes-vpvqe/ (accessed 27 October 2024).

Halevi, T., Memon, N., Lewis, J., Kumaraguru, P., Arora, S., Dagar, N., Aloul, F., *et al.* (2016), *Cultural and Psychological Factors in Cyber-Security*, doi: 10.1145/3011141.3011165.

Havlicek, L.L. and Peterson, N.L. (1976), “Robustness of the Pearson Correlation against Violations of Assumptions”, *Perceptual and Motor Skills*, SAGE Publications Inc, Vol. 43 No. 3_suppl, pp. 1319–1334, doi: 10.2466/pms.1976.43.3f.1319.

“Hofstede’s Globe”. (2015), *Geert Hofstede*, available at: https://geerthofstede.com/hofstedes-globe/ (accessed 29 October 2024).

Johnson, K. (2017), *Better Safe than Sorry: The Relationship between Locus of Control, Perception of Risk, and Cyber Misbehaviors*, M.A., University of South Florida, United States -- Florida.

Jones, J.G. and Simons, H.W. (2017), *Persuasion in Society*, 3rd ed., Routledge, New York, doi: 10.4324/9781315739816.

Jones, K.S., Armstrong, M.E., Tornblad, M.K. and Siami Namin, A. (2021), “How social engineers use persuasion principles during vishing attacks”, *Information & Computer Security*, Emerald Publishing Limited, Vol. 29 No. 2, pp. 314–331, doi: 10.1108/ICS-07-2020-0113.

Lee, S. and Liang, Y. (2015), “Reciprocity in Computer–Human Interaction: Source-Based, Norm-Based, and Affect-Based Explanations”, *Cyberpsychology, Behavior and Social Networking*, Vol. 18, doi: 10.1089/cyber.2014.0458.

Mahmoud, S., Abo Alez, R. and EL-Refai, F. (2017), “PERSUASION BASED RECOMMENDATION SYSTEM”, *Journal of Al-Azhar University Engineering Sector*, Vol. 12 No. 44, pp. 894–899, doi: 10.21608/auej.2017.19199.

Markus, H.R. and Kitayama, S. (1991), “Culture and the self: Implications for cognition, emotion, and motivation.”, *Psychological Review*, Vol. 98 No. 2, pp. 224–253, doi: 10.1037/0033-295X.98.2.224.

Mitnick, K. and Simon, W. (2002), “The Art of Deception: Controlling the Human Element of Security”.

Mollazehi, A., Abuelezz, I., Barhamgi, M., Khan, K.M. and Ali, R. (2024), “Do Cialdini’s Persuasion Principles Still Influence Trust and Risk-Taking When Social Engineering is Knowingly Possible?”, in Araújo, J., de la Vara, J.L., Santos, M.Y. and Assar, S. (Eds.), *Research Challenges in Information Science*, Springer Nature Switzerland, Cham, pp. 273–288, doi: 10.1007/978-3-031-59465-6_17.

Muhanad, A., Haris, R., Abouelezz, I., Barhamgi, M., Ali, R. and Khan, K.M. (2024), “Do Personality Traits Really Impact Susceptibility to Persuasion in Social Engineering? A Study Among UK and Arab Samples”, 2 September, doi: 10.21203/rs.3.rs-4902235/v1.

Murphy, P.K., Long, J.F., Holleran, T.A. and Esterly, E. (2003), “Persuasion online or on paper: a new take on an old issue”, *Learning and Instruction*, Vol. 13 No. 5, pp. 511–532, doi: 10.1016/S0959-4752(02)00041-5.

Oyibo, K. and Vassileva, J. (2019), “The relationship between personality traits and susceptibility to social influence”, *Computers in Human Behavior*, Vol. 98, pp. 174–188, doi: 10.1016/j.chb.2019.01.032.

Pal, M. and Bharati, P. (2019), “Introduction to Correlation and Linear Regression Analysis”, in Pal, M. and Bharati, P. (Eds.), *Applications of Regression Techniques*, Springer, Singapore, pp. 1–18, doi: 10.1007/978-981-13-9314-3_1.

Perlroth, N. (2013), “Hackers in China Attacked The Times for Last 4 Months”, *The New York Times*, 31 January.

Petty, R. and Cacioppo, J. (1986), “The Elaboration Likelihood Model of Persuasion”, *Advances in Hydroscience*, Vol. 19, pp. 124–205.

Roberts, S.A. (2021), *Exploring the Relationships Between User Cybersecurity Knowledge, Cybersecurity and Cybercrime Attitudes, and Online Risky Behaviors*, Ph.D., Northcentral University, United States -- California.

Rohan, R., Funilkul, S., Pal, D. and Chutimaskul, W. (2021), “Understanding of Human Factors in Cybersecurity: A Systematic Literature Review”, *2021 International Conference on Computational Performance Evaluation (ComPE)*, presented at the 2021 International Conference on Computational Performance Evaluation (ComPE), pp. 133–140, doi: 10.1109/ComPE53109.2021.9752358.

Ruhl, C. (2023), “Implicit Bias: What It Is, Examples, & Ways to Reduce It”, 2 August, available at: https://www.simplypsychology.org/implicit-bias.html (accessed 29 October 2024).

Sagarin, B.J., Cialdini, R.B., Rice, W.E. and Serna, S.B. (2002), “Dispelling the illusion of invulnerability: The motivations and mechanisms of resistance to persuasion”, *Journal of Personality and Social Psychology*, American Psychological Association, Washington, US, Vol. 83 No. 3, pp. 526–541, doi: 10.1037/0022-3514.83.3.526.

Schmidt, F.L. and Hunter, J.E. (1996), “Measurement error in psychological research: Lessons from 26 research scenarios”, *Psychological Methods*, American Psychological Association, US, Vol. 1 No. 2, pp. 199–223, doi: 10.1037/1082-989X.1.2.199.

Schoenmakers, K., Greene, D., Stutterheim, S., Lin, H. and Palmer, M.J. (2023), “The security mindset: characteristics, development, and consequences”, *Journal of Cybersecurity*, Vol. 9 No. 1, p. tyad010, doi: 10.1093/cybsec/tyad010.

Seidel-Fischer, J., Trifunovic-Koenig, M., Gerber, B., Otto, B., Bentele, M., Fischer, M.R. and Bushuven, S. (2024), “Interaction between overconfidence effects and training formats in nurses’ education in hand hygiene”, *BMC Nursing*, Vol. 23 No. 1, p. 451, doi: 10.1186/s12912-024-02020-w.

Senthilnathan, S. (2019), “Usefulness of Correlation Analysis”, *SSRN Electronic Journal*, doi: 10.2139/ssrn.3416918.

Sharma, M. (2021), “This phishing campaign uses a sneaky attachment scam”, *TechRadar*, 9 April.

Siddiqi, M.A., Pak, W. and Siddiqi, M.A. (2022), “A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures”, *Applied Sciences*, Multidisciplinary Digital Publishing Institute, Vol. 12 No. 12, p. 6042, doi: 10.3390/app12126042.

Smith, E.R., Mackie, D.M. and Claypool, H.M. (2014), *Social Psychology: Fourth Edition*, 4th ed., Psychology Press, New York, doi: 10.4324/9780203833698.

Szűcs, K.R., Tick, A. and Reicher, R.Z. (2024), “Applying attitude theory to determine user security approaches”, *Serbian Journal of Management*, Vol. 19 No. 1, pp. 133–148, doi: 10.5937/sjm19-45280.

The State of Cyber Defense 2023: Detection and Response Maturity Model. (2023), , Kroll.

Toro-Jarrin, M.A., Pazos, P. and Padilla, M.A. (2024), “It is not only about having good attitudes: factor exploration of the attitudes toward security recommendations”, *Journal of Cybersecurity*, Vol. 10 No. 1, p. tyae011, doi: 10.1093/cybsec/tyae011.

Tsinganos, N., Sakellariou, G., Fouliras, P. and Mavridis, I. (2018), “Towards an Automated Recognition System for Chat-based Social Engineering Attacks in Enterprise Environments”, *Proceedings of the 13th International Conference on Availability, Reliability and Security*, presented at the ARES 2018: International Conference on Availability, Reliability and Security, ACM, Hamburg Germany, pp. 1–10, doi: 10.1145/3230833.3233277.

Vargas-Sánchez, A., Plaza-Mejía, M.Á. and Porras-Bueno, N. (2016), “Attitude”, in Jafari, J. and Xiao, H. (Eds.), *Encyclopedia of Tourism*, Springer International Publishing, Cham, pp. 58–62, doi: 10.1007/978-3-319-01384-8_11.

Wall Emerson, R. (2023), “Regression and Effect Size”, *Journal of Visual Impairment & Blindness*, SAGE Publications Inc, Vol. 117 No. 2, pp. 191–192, doi: 10.1177/0145482X231166596.

Wall, H.J., Campbell, C.C., Kaye, L.K., Levy, A. and Bhullar, N. (2019), “Personality profiles and persuasion: An exploratory study investigating the role of the Big-5, Type D personality and the Dark Triad on susceptibility to persuasion”, *Personality and Individual Differences*, Vol. 139, pp. 69–76, doi: 10.1016/j.paid.2018.11.003.

Wang, P.A. (2013), “Assessment of Cybersecurity Knowledge and Behavior: An Anti-phishing Scenario”, *Proc. IEEE Int. Conf. Internet Monitor. Protection (ICIMP)*, pp. 1–7.

Wang, Z., Zhu, H. and Sun, L. (2021), “Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods”, *IEEE Access*, presented at the IEEE Access, Vol. 9, pp. 11895–11910, doi: 10.1109/ACCESS.2021.3051633.

Williams-Banta, P.E. (2019), *Security Technology and Awareness Training; Do They Affect Behaviors and Thus Reduce Breaches?*, Ph.D., Northcentral University.

Wilson, M., McDonald, S., Button, D. and McGarry, K. (2023), “It Won’t Happen to Me: Surveying SME Attitudes to Cyber-security”, *Journal of Computer Information Systems*, Taylor & Francis, Vol. 63 No. 2, pp. 397–409, doi: 10.1080/08874417.2022.2067791.

Zalake, M., Siqueira, A.G. de, Vaddiparti, K. and Lok, B. (2021), “The effects of virtual human’s verbal persuasion strategies on user intention and behavior”, *International Journal of Human-Computer Studies*, Vol. 156, p. 102708, doi: 10.1016/j.ijhcs.2021.102708.