Journal of Posthumanism

2025

Volume: 5, No: 6, pp. 1013–1026

ISSN: 2634-3576 (Print) | ISSN 2634-3584 (Online)

posthumanism.co.uk

DOI: https://doi.org/10.63332/joph.v5i6.2175

Social Engineering as an Intermediate Variable between Methods of Persuasion and Electronic Deception from the Point of View of Victims of Cybercrime

Al-Nafisa, Shaden Ali[1], Khatatbeh, Yahya M[2]

Abstract

The study aimed to reveal the role of social engineering as a mediating variable between methods of persuasion and electronic deception from the point of view of victims of cybercrime. The sample consisted of (164) male and female students who were victims of cybercrime in one of the university colleges in the Kingdom of Saudi Arabia, who were selected by a simple random sample method. The study used the social engineering scale (AbdelTawab, 2021), electronic deception scale (Mangoud & Ali, 2022) And the scale of persuasion methods (Kaptein et al., 2012). The data showed that the average social engineering exceeded the hypothetical average by 41.9%, outperforming the average phishing (16.6%), while the persuasion was less than expected by 26.5%, suggesting that criminals rely heavily on systematic psychological influence rather than traditional persuasive arguments, analyses have demonstrated a strong correlation between persuasion methods and cyber deception. (t = 0.890), reinforcing the hypothesis that persuasion is a precursor to deception. When the impact of social engineering was isolated, the correlation decreased to (t = 0.280), which confirms its role as a key intermediary variable in this relationship, and the results also showed the ability of high social engineering in predicting persuasion methods. (R^2 = 0.898) and phishing (R^2 = 0.931), with the human dimension emerging as the most influential (Beta = 0.637 in persuasion, and Beta = 0.628 In deception), compared to the technical dimension. Regression models and strong statistical significance confirm that the combination of emotional impact and fraudulent techniques forms a fertile environment for victim occurrence, and finally, three-dimensional representation illustrates how the increase of both dimensions (Human & Technical) In social engineering, it leads to a significant escalation in the level of deception, which supports the conclusion that this psychological strategy is the most effective tool in modern cybercrime operations. Social engineering is the hinge that transforms persuasion methods into effective cyber deception for victims of cybercrime.

Keywords: *Social engineering, Cyber deception, Persuasion techniques, Victims of cybercrime*

Introduction

Social engineering is an effective psychological tool that links cyber persuasion and deception, with victims of cybercrime suggesting that the deception they experienced was more emotional than technical.. Illustrates both (Butavicius et al., 2016; Workman, 2008) that false trust and power are exploited to convince victims, while showing (Khadka et al., 2023)The use of classical persuasion methods increases the effectiveness of attacks. Even security-trained personnel, he noted (Halevi et al., 2013) Not Immune from these methods, which reinforces the importance of understanding the role of social engineering as an intermediate variable, suggests (Van Der Zee et al., 2019) indicates that attackers adapt their messages to suit the victim's weaknesses, making deception seem natural. This is confirmed by studies (Albladi & Weir, 2020)About the impact of context, such as employment or financial services. Between (Chen et al., 2010)The way the

[1] Imam Mohammad Ibn Saud Islamic University (IMSIU), Email: 444011427@sm.imamu.edu.sa

[2] Imam Mohammad Ibn Saud Islamic University (IMSIU), Email: ymkattabh@imamu.edu.sa

message is presented outweighs its content in its ability to convince. Therefore, victims do not experience a single moment of deception, but rather undergo a gradual manipulation process based on trust.

Cybercrime, which includes various forms of cybercrime, has become a major concern in the digital age. They include traditional crimes adapted to the electronic environment and new crimes enabled by technology(Ballou, 2010)، The banking sector is particularly vulnerable, with ATM fraud, money laundering and credit card fraud being common threats. (Pasricha & Mehrotra, 2014; Rao, 2019)، The internet has created new opportunities for criminals to hide their identities and commit sexual and financial crimes. (Ryder & Reid, 2012) The theory of routine activity explains the occurrence of cybercrime, attributing this to the increase in the number of Internet users and technology literacy. Governments have introduced legislation to combat cybercrime, but its effectiveness is debatable with rapid technological advancement. (Yar, 2012) To mitigate cybercrime in the banking sector, the use of modern technology and the presence of trusted employees is critical However, estimating the prevalence of cybercrime and associated harms remains a challenge due to methodological difficulties. (Rao, 2019), considered Cybercrime is a common phenomenon in the world. It is a set of activities carried out by individuals by disrupting networks, stealing important and private data and documents for others, hacking bank details and accounts, and transferring money to their own accounts. The importance of cybercrime, especially online, has increased with the increasing importance of computers in commerce, entertainment and government(Brinkhof, 2024)، Cybercrime, also known as computer crime, is the use of a computer as a tool to achieve illegal ends, such as fraud, child pornography and intellectual property, identity theft, and invasion of privacy. (Sherman, 2000) These crimes range from fraud and identity theft to child pornography and cyberterrorism. (Al-Khater et al., 2020) The increasing diversity and complexity of cybercrime strategies pose significant challenges to understanding risks and developing effective preventive policies. (Sabillon et al., 2016) Cybercrime can have serious consequences, including economic disruption, psychological distress, and threats to national security, and despite the focus on cyberattacks, many cybercrimes are traditional crimes facilitated by technology. (Zhang et al., 2012) The proliferation of recurrent cybercrime highlights the need for enhanced protection and research in this area.

and exploits social engineering (THE AVENUE) In the field of cybersecurity human vulnerabilities to penetrate information systems (Burda et al., 2021)، It relies on persuasion techniques to manipulate victims to divulge sensitive information, and social engineering is a taboo subject in our contemporary society.. It involves using social skills to obtain usernames, passwords, and credit card data, or hacking or changing an entity's information and systems. (Wang et al., 2021), the Social engineering methods are versatile, used by highly adept and adaptable people. This technology exploits the innate nature of humans to manipulate and obtain sensitive information, and convince people to reveal it, using exceptional communication skills.. (Alotayan, 2024) Five models of persuasion have been identified, based on: Simplicity, interest, contradiction, trust, and empathy, exploiting the main factors that predispose people to fall victim to social engineering attacks, such as greed, self-interest, guilt, or ignorance. It is known that security is measured by the strength of the weakest link in it (Individuals)Therefore, beyond technical measures, staff training is key to success in defending against such attacks.. (Greavu-Serban & Serban, 2014) Social engineering attacks often use Salini's principles of persuasion, leveraging psychological biases and social hierarchies to influence decision-making. (Wantenaar, 2022) The effectiveness of social engineering lies in its ability to exploit human tendencies towards trust and social norms, making it a key element in many cyberattacks. (Burda et al.,

2021) While traditional cybersecurity focuses on technical vulnerabilities, social engineering targets the human element, which is often the weakest link in security systems. (Greavu-Serban & Serban, 2014), requires Understanding service software is a multidimensional approach, taking into account persuasion, manufacturing and data collection aspects, and to counter service software threats, organizations must prioritize employee training along with technical measures (Hadnagy, 2010). Due to a lack of analytical concepts, research on social engineering has difficulties explaining its success. In such explanations, too much emphasis is placed on the psychological characteristics of the victim, although this type of explanation covers only a small part of social engineering cases. (Burda et al., 2021)

description (Mitnick & Simon, 2003) Stages of implementing social engineering attacks It is a four-stage attack cycle: Research: It includes gathering information about the target, developing relationship and trust: different types of social engineering techniques are deployed at this stage to ensure the victim's trust in the attacker, and exploiting trust: attackers rely on human behavior to exploit the trust gained, steal the required information surreptitiously, and use the information. According to (Montañez et al., 2020) Cognitive psychologists often consider information processing to be the primary function of the brain, as different types of information processing generate behavior together. Cognition is one of the types of abstract information processing that is carried out by neurons in the brain, and there are short-term cognitive factors that operate at relatively short intervals of time (minutes to hours), and have been extensively studied because of their negative impact on performance and their cause to promote the exploitation of victims through social engineering.

Aimed at studying (Qwaisy & Alhalwany, 2024) To know the prevalence of electronic fraud among rural university youth. The questionnaire was applied to (200) students, the total average degree of prevalence of electronic fraud images among rural university youth was (2.32), and the top reasons that lead to their fall under electronic fraud were: the wrong use of Internet sites, and access to unsafe sites. The results also indicated that (68%) of the respondents came within the middle category in terms of their knowledge of the rules of safe use of social media. The study (Junger et al., 2023) to the detection of cyber phishing by actual victims, as well as People who were about to fall victim، From their point of view The sample consisted of (1201) participants from the United States, with an average age (53) years, the results indicated noted that people who were about to fall victim noticed that the scammers used specific methods، As: Promote a sense of urgency in messages or calls, as well as exploit trust by presenting themselves as trusted or known people، It has also been noted that some scammers sought to create fear to push victims to make quick decisions without adequate verification.، The detection strategies possessed by the participants contributed، As: Suspicion and distrust, knowledge of deception methods, technical expertise، in reducing the likelihood of them falling victims.

The study aimed at (Anesa, 2020) into analysis methods Persuasion Used in emotional deception, and understand the nature of deceptive speech Add to Identify the psychological and linguistic factors that make victims fall into the trap. It included (26) groups of real fraudulent conversations and(43) Fraudulent message prepared Already. The results showed Poor security awareness is not the only factor for the success of deception, as victims fall into the trap because of methods Strong persuasion. The results of the study indicated Scammers use psychological and rhetorical techniques aimed at reducing victims' ability to validate information due to the influence of strong emotions, leading to errors in judgment and discrimination.، The results confirmed that The victim does not fall victim to deception Not only because of a lack of security knowledge, but because scammers succeed in creating a rhetorical environment that makes the victim less able to resist requests. Scams follow a recurring pattern that includes building trust, boosting emotion, and then incremental financial demands.. The (Jones et al., 2021) A study aimed at Explore how to use persuasion principles during phishing attacks, with a view to Understand the repetitive patterns of these principles and analyze their repetition and use by attackers. The study sample consisted of (86) attacks collected from various international sources, and the results indicated into That attackers in real-life attacks of social engineering rely on known and repeated patterns From the methods of persuasion She explained that these attacks do not rely on chance, but on pre-studied techniques, which makes it possible to analyze the methods. and predict their use, the results showed A difference between the behavior of attackers via email and phone, where the use of "Social Proof" is more pronounced in phone attacks, reflecting clear preferences in social engineering strategies according to for the scenario. This methodological approach enhances the possibility of prior analysis and prediction of the persuasion methods used. The (Gámez-Guadix et al., 2018)To find out the relationship between adult use of online sexual grooming and persuasion techniques for adolescents. The sample consisted of (196) Spanish adolescents, males and females, between the ages of (12) and (15) years. The most prominent results showed that I do not Approximately two out of every three adolescents (65.6)%) that they Goals for at least one type of methods Persuasion that he uses Adults in online sexual grooming. It also showed that girls are more exposed to persuasion methods than adults than boys. In addition، Deception and bribery have been associated with higher rates of sexual temptation, which in turn has led to an increase in abusive sexual interactions. The results also showed that the most commonly used persuasion technique is admiration.

Hypotheses

H1 There is a high level of occurrence of social engineering, electronic deception, and persuasion techniques among victims of cybercrime

H2 There is a statistically significant relationship between persuasion techniques and electronic deception from the perspective of victims of cybercrime

H3 Controlling for social engineering significantly affects the correlation between persuasion techniques and electronic deception from the perspective of victims of cybercrime

H4 Social engineering significantly predicts the use of persuasion techniques and electronic deception against victims of cybercrime.

Materials and Methods

Participants

The study population consisted of all students enrolled in the College of Arts and Sciences in the Kingdom of Saudi Arabia, estimated at (4,807) male and female students, according to the latest statistics for the year (2024 AD). The population includes students enrolled in the bachelor's degree (3,341) male and female students, and diploma (1,466) male and female students, aged (18 years and older). The study sample was selected from among the population members according to the simple random sample methodology, with the sample size amounting to (164) male and female students who were victims of cybercrimes in the diploma and bachelor's degrees. The sample was distributed as follows: (77) male students and (87) female students, taking into account the application of sample criteria, which included the student being officially registered in the College of Arts and Sciences in Al-Rass during the study period in the second semester of the academic year 2024-2025 AD.

Instrument

A. Social Engineering Scale: The scale of university youth attitudes towards social engineering was used (AbdelTawab, 2021) It consists of (32) items distributed on the dimensions of social engineering on a technical basis, and social engineering on a human basis. Paragraphs are corrected according to the Likert triple scale. The validity of the phenotypic scale and content was verified by the referees in this current study, as the results of the Cronbach alpha coefficient (Cronbach's Alpha) (0.905), reflecting a high level of stability of the scale in this study.

B. Electronic Deception Meter The study relied on an electronic scale for university youth on planning to develop university youth's awareness of the dangers of cybercrime, a future vision" (Mangoud & Ali, 2022) Which consists of (77) items distributed on three axes: dimensions of cybercrime, obstacles that limit awareness, and proposals for awareness development. Paragraphs are corrected according to the Likert triple scale. The validity of the phenotypic scale and content was verified by the referees in this current study, as the results of the Cronbach alpha coefficient (Cronbach's Alpha) (0.956), reflecting a high level of stability of the scale in this stu

C. Scale of persuasion methods: The persuasion methods scale was used (Kaptein et al., 2012) and component From (26) items Distributed in six dimensions according to the Salini model of persuasion. Paragraphs are corrected according to the Likert heptathlon scale. The validity of the phenotypic scale and content was also verified by the referees in this current study, and the results of the Cronbach alpha coefficient (Cronbach's Alpha) (0.957) high level of stability in this context.

Results

1. The incidence of social engineering, online deception, and persuasion techniques among cybercrime victims

Figure (1) shows a close comparison between the actual and hypothetical averages for social engineering, online deception, and persuasion techniques among cybercrime victims, with the differences shown as percentages. It is clear that the social engineering average exceeded the expected average by 41.9%, reflecting the perpetrators' heavy reliance on psychological influence strategies to lure victims. The online deception average also exceeded the hypothetical average by 16.6%, indicating the strength of the fraudulent methods used. In contrast, the persuasion techniques average was 26.5% lower than the hypothetical average, which may be understood as victims becoming more aware of traditional persuasive arguments compared to emotional and targeted deception methods. This disparity in differences highlights the pivotal role of social engineering as an effective mediator in the transition from persuasion to deception in the digital environment.

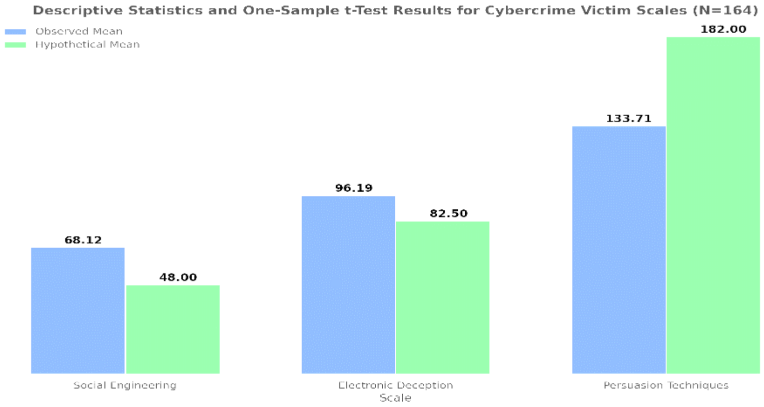
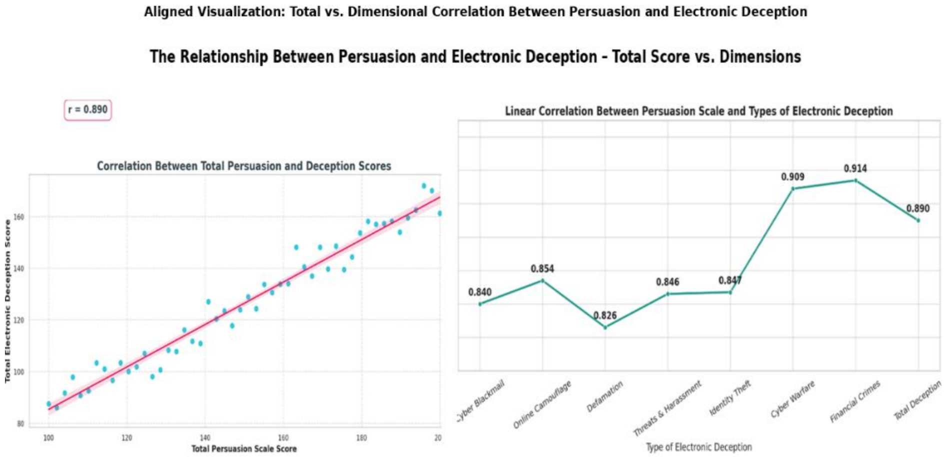


Figure (1) shows the arithmetic averages of social engineering, electronic deception, and persuasion methods among victims of electronic crimes**.**

2. The Relationship between Persuasion Methods and Cyber Deception from the Perspective of Cybercrime Victims

The study results showed a strong positive correlation between the total score on persuasion methods and the total score on the cyberaddiction scale, with a correlation coefficient of (r = 0.890). This indicates that individuals' increased use or exposure to persuasion methods is associated with an increased likelihood of being subjected to cyberaddiction. This result reflects theoretical consistency with the hypothesis that cybercrime is not solely dependent on technological tools, but rather is gradually built through systematic psychological influence (Figure 2).



The results of the statistical analysis shown in the left figure show a strong direct correlation between the total score of persuasion methods and the total score of cybercrime deception among cybercrime victims. The correlation coefficient (r = 0.890) is clear evidence that individuals with a high level of persuasion significantly increase their likelihood of being exposed to cyberaddiction. This indicates that persuasion constitutes a primary psychological input that facilitates the process of manipulation and deception by perpetrators.

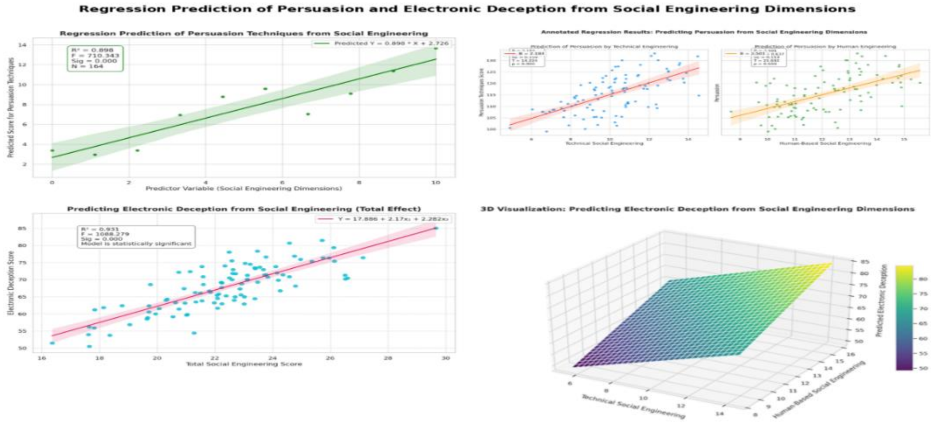
The right figure displays the relationship between the persuasion scale and each dimension of cyberaddiction separately. The results revealed varying strengths of correlation, with financial crimes (r = 0.914) and cyberwarfare (r = 0.909) recording the highest correlations, indicating that these types of deception rely heavily on complex and organized persuasion methods. In contrast, the lowest correlation was with the defamation and slander dimension (r = 0.826), indicating that this type of deception relies more on direct attacks than gradual trust building. The correlation coefficients between the dimensions showed high values, reflecting the homogeneity of the elements and their connection to their theoretical concept. This enhances the validity of the scales and lends credibility to the scientific interpretation of the extracted results. Regarding the correlations between the total score of persuasion methods and the dimensions of electronic deception, the results revealed strong positive correlations ranging between 0.826 and 0.914. The "impersonation" dimension achieved a high correlation (r = 0.847), reflecting the nature of this type of behavior, which requires building initial trust through persuasion before deception.

3. The Impact of Social Engineering Isolation on the Correlation Coefficients of Persuasion and Cyber Deception Methods from the Perspective of Cybercrime Victims

The results shown in **Table (1)** indicate a strong positive correlation between persuasion methods and cyber deception before the isolation process. The correlation coefficient reached 0.890 at the significance level of 0.01, indicating that the relationship was positive and strong. However, after isolating the effect of social engineering, the correlation coefficient decreased to 0.280 at the significance level of 0.05, indicating that the relationship had become weak. This significant decrease indicates that social engineering played a major role as a mediating variable in strengthening the relationship between persuasion methods and cyber deception.

Scale of persuasion methods		**Variable**
After isolating the effect	**Before insulating the effect**	
* 0.280^{*}	0.890^{**}	Electronic Deception Meter

4. How do social engineering dimensions contribute to predicting the levels of persuasion and electronic deception among victims of cybercrime?



The results of the regression analysis shown in the four figures reveal the strong influence of social engineering dimensions in predicting both persuasion and electronic deception methods among cybercrime victims, using accurate and highly significant statistical models.

First: Predicting persuasion methods. Figure 1 shows that social engineering explains 89.8% of the variance in persuasion methods, as indicated by the coefficient of determination $R^2 = 0.898$ and the simple predictive equation used. The results also demonstrated high statistical significance for the model, with the calculated F value reaching 710.343 at a significance level of (Sig = 0.000), confirming the validity of the model and its predictive ability. Second: Predicting persuasion through the technical and human dimensions. The second image shows that the two dimensions together form a robust model, with the human dimension having a higher influence coefficient (B = 2.501, Beta = 0.637), and the technical dimension having a relatively lower influence (B = 2.184, Beta = 0.431). The adopted equation is: Persuasion = 2.184×Technical + 2.501×Human + 63.261.

Third: Predicting electronic deception (total). The third image shows that the model explains 93.1% of the variance in electronic deception ($R^2 = 0.931$), which is a very high figure. The model is statistically significant (Sig = 0.000, F = 1088.279), and is expressed by the equation: Deception = 2.17×Technical + 2.282×Human + 17.886.

Fourth: Three-dimensional representation (3D) The final figure reinforces the interaction between the two dimensions of social engineering, showing how any combined increase in both dimensions leads to a significant increase in cyber deception scores. This type of representation is visually supportive of predictive models, especially in understanding the complex interaction between variables. These values indicate that both dimensions are statistically significant, but the human dimension has a stronger effect (Beta = 0.628), reflecting the greater importance of emotional manipulation and direct human contact in paving the way for cyber deception, more than simply exploiting technical vulnerabilities. The presented 3D figure translates this equation into a visual representation showing how increases in both dimensions lead to increased cyber deception. Note that the prediction surface clearly rises as the values in both dimensions of social engineering increase together. The predictive equation is as follows: Cyber Deception = 17.886 + 2.17 × (Technical Socinianizing) + 2.282 × (Human Socinianizing)

Discussion

The results of the graph reflect significant differences between the actual means observed in the study sample (N=164) and the theoretically hypothesized means. These differences reveal clear trends that reflect the nature of the real-life experience of cybercrime victims compared to what is expected or assumed. Regarding the social engineering scale, the actual mean was 68.12, significantly exceeding the hypothetical mean of 48.00. This indicates that cybercrime victims are actually exposed to a high level of systematic manipulation, whether through technical techniques (such as fake links) or through fraudulent human communication (such as impersonation or emotional blackmail). This result indicates that perpetrators do not rely solely on technical means, but rather employ targeted psychological methods to mislead the victim, which reinforces the importance of studying social engineering as a systematic behavior, not just as a technical tool. On the online deception scale, the actual mean (96.19) was higher than the hypothetical mean (82.50), reflecting that victims are not only exposed to deception attempts, but actually fall victim to them. This result confirms that the online environment is an active arena for deception, which takes multiple forms (financial, personal, informational), and is practiced in ways that demonstrate the evolution of cybercrime methods and their integration with social engineering. In contrast, the persuasion methods scale recorded a different result, with the actual mean (133.71) being lower than the hypothetical mean (182.00). This may indicate two key points: First, victims are not sufficiently aware that the methods used against them were part of a hidden and systematic persuasion process, and second, some persuasion methods may have occurred indirectly or intangibly, making them difficult for non-experts to perceive.

These results are consistent with the study of (Atkins & Huang, 2013) Which pointed out that social engineering is mainly used in electronic deception by exploiting human weaknesses and psychological manipulation of victims, and the study of (Qwaisy & Alhalwany, 2024) Which found the prevalence of electronic fraud among university youth reached (2.32) out of (3) degrees. On the other hand, all studies agree that the human side is the weakest link in cybersecurity, and that technical solutions alone are not enough without enhancing psychological and behavioral awareness with persuasion methods and social engineering that pave the way for electronic deception. (Black & Sarno, 2023; Chapagain et al., 2024; Schmitt & Flechais, 2024; Wang et al., 2020) Studies show that persuasion methods such as scarcity, reciprocity, social consensus, and commitment are cleverly used in fraudulent emails, fake advertisements, and other methods, often passing unnoticed by the victim. As a study shows (The Influence of Time Pressure – SAGE, 2023) Victims' ability to discern deceptive messages is significantly reduced when these principles are combined with psychological or emotional stress.

The results of the study indicate a strong positive correlation between the use of persuasion methods and exposure to electronic deception, where the correlation coefficient (t = 0.890). This shows that individuals who are exposed to advanced persuasion techniques are more likely to fall victim to cybercrime. This relationship is particularly evident in financial crime (t = 0.914) Electronic Warfare (t = 0.909), suggesting that these types of crimes rely heavily on complex persuasion techniques, these findings are consistent with the scientific literature emphasizing the role of persuasion methods in facilitating cyber deception. For example, a study shows (Rajivan & Gonzalez, 2018) Phishing messages rely on persuasion strategies such as urgency and plagiarism to increase the effectiveness of the attack. . As a study suggests (Brinkhof, 2024)Phishing messages use techniques such as pretending to be trusted sources and creating a sense of urgency to prompt victims to take action without thinking.

A study published in the journal (Siddiqi et al., 2022)Techniques Social engineering, such as phishing and electronic sexual blackmail, relies on persuasion and psychological manipulation to achieve its goals.(Ahe, 2022) Victims of cybercrime suffer negative psychological effects, such as: anxiety, depression and loss of self-confidence, especially when the perpetrator is known to the victim or there was intense communication before the crime . This reinforces the hypothesis that persuasion constitutes a psychological input that facilitates manipulation and deception by offenders, and it can be said that the results of the study are consistent with the scientific literature that emphasizes the pivotal role of persuasion methods in facilitating electronic deception.. This points to the importance of developing awareness and training strategies that focus on enhancing awareness of the persuasion techniques used in cybercrime, which helps individuals to identify and effectively counter deception attempts..(Bustio-Martínez et al., 2024; Khadka, 2024; Khadka et al., 2023; Koddebusch, 2022) It showed how persuasion techniques are systematically used in phishing attacks, reinforcing the need to educate individuals about these methods and develop defensive strategies based on understanding the psychology of victims and the methods of attackers.. The results of the current study also reveal the strength of the impact of the dimensions of social engineering. (Human and technical dimension) In predicting both methods of persuasion and electronic deception, which is consistent with the orientations of many previous studies that stressed the importance of these dimensions in understanding the mechanisms of falling victim to cybercrime.

First of all: The power of predicting persuasion methods through social engineering (R^2 = 0.898) The results of the study show that social engineering explains approximately 90% of variation in persuasion methods, suggesting a pivotal role for psychosocial and technical characteristics in shaping this behavior. This finding is supported by my findings. study (Hadnagy, 2010) who pointed out that emotional content and false urgency are key catalysts for persuasion within

secondly: The superiority of the human dimension in predicting persuasion and electronic deception (Beta human > Beta technical) The results showed that the human dimension has a greater impact than the technical dimension in both persuasion (Beta = 0.637) and phishing (Beta = 0.628), which indicates the importance of the psychosocial factor in the manipulation of victims and is consistent with the results of the study(Jagatic et al., 2007) Benoit That messages designed based on real social information (Human dimension) They were more effective at fooling users than the general ones.

thirdly: Significance of the interactive model (3D visualization) in promoting complex understanding The three-dimensional drawing presented by the study enhances the explanatory value of the statistical model, as it clearly shows that the interaction between the technical and human dimensions leads to a significant escalation in cyber deception, and the evidence from previous studies supports the validity of the findings of the current study. (Khadka, 2024; Schmitt & Flechais, 2024). They all agree that social engineering, especially the human dimension, plays a crucial role in enhancing the effectiveness of both cyber persuasion and deception.. This consensus reinforces confidence in the validity of the statistical models used, and emphasizes the importance of developing preventive strategies that focus on enhancing individuals' awareness of the psychological and social behaviors that are exploited in these crimes, not just technical defenses. Understanding social engineering mechanisms and methods effectively contributes to the development of predictive models capable of identifying risk factors associated with cyber deception. (Chapagain et al., 2024)These models, which rely on analyzing human emotions and cognitive biases, can enhance the effectiveness of prevention strategies and increase individuals' awareness of the dangers of psychological manipulation, reducing their likelihood of being exposed to deceptive cyberattacks. (Jagatic et al., 2007; Workman, 2008; Wright & Marett, 2010).

Recommendations

Include persuasion and social engineering methods in bepraising awareness programs, with the aim of enhancing individuals' understanding of how these methods affect their decisions, through the efforts of social, media and educational institutions.

Conduct additional studies focused on understanding the role of social engineering in the impact of persuasion techniques on cyber deception by raising awareness of how bepraising occurs and ways to prevent it.

Develop predictive models based on social engineering principles to identify the most common cyber deception methods, and contribute to the development of effective preventive strategies to reduce risks, with the possibility of integrating artificial intelligence techniques to enhance prediction accuracy and protection effectiveness.

Limitation

This study has several strengths, most notably the rigor of its methodological design. It used standardized and highly reliable tools (such as the Social Engineering Scale, the Electronic Deception Scale, and the Persuasion Methods Scale), in addition to relying on a realistic sample of cybercrime victims, which enhances the validity and relevance of the results. The study also presented advanced statistical analysis using regression models and three-dimensional analysis of variance, which added interpretive depth to the relationships between variables. The results demonstrated the importance of the human dimension in social engineering as a crucial factor in predicting deception and persuasion, a qualitative addition to the field of technical psychology.

However, some weaknesses are noted in the study, such as the fact that the sample was limited to students from a single college in Saudi Arabia, which may limit the generalizability of the results to broader population segments. Furthermore, the reliance on a self-reporting method may expose the data to biases of memory or the influence of personal experiences. In addition, despite the theoretical diversity in references, the study did not conduct longitudinal comparisons or differences between genders or age groups, which deprives it of some analytical depth in explaining individual differences in exposure to and influence by persuasion and social engineering methods.

Finding Statement

The authors extend their appreciation to the Deanship of Scientific Research at Imam Mohammad Ibn Saud Islamic University (IMSIU) for funding and supporting this work through the Graduate Students Research Support Program (IMSIU-GSRSP).

References

AbdelTawab, T. A. (2021). University youth's attitudes towards social engineering and its relationship to cultural identity. *Journal of the College of Social Work for Social Studies and Research*, *22*(Issue No. 22, Part 1), 485-529 .

Ahe, L. v. d. (2022). *Mental Wellbeing and Cybercrime (The Psychological Impact of Cybercrime on the Victim)* University of Twente .[

Al-Khater, W. A., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020). Comprehensive review of cybercrime detection techniques. *IEEE access*, *8*, 137293-137311 .

Albladi, S. M., & Weir, G. R. (2020). Predicting individuals' vulnerability to social engineering in social networks. *Cybersecurity*, *3*(1), 7 .

Alotayan, T. (2024). Awareness of Social Engineering Attacks and their Relation to the Ability to Persuade among users of Social Networking Sites. *Journal of Ecohumanism*, *3*(7), 2580–2592-2580–2592 .

Anesa, P. (2020). Lovextortion: Persuasion strategies in romance cybercrime. *Discourse, Context & Media*, *35*, 100398 .

Atkins, B., & Huang, W .(2013) .A study of social engineering in online frauds. *Open Journal of Social Sciences*, *1*(03), 23 .

Ballou, S. (2010). *Electronic crime scene investigation: A guide for first responders*. Diane Publishing .

Black, J., & Sarno, D. M. (2023). The Influence of Time Pressure and Persuasion Principles on Phishing Detection. Proceedings of the Human Factors and Ergonomics Society Annual Meeting ,

Brinkhof, D. (2024). *Understanding the Human Dimension: The Role of Persuasion and Psychological Factors in Cyberattack Vulnerability* University of Twente .[

Burda, P., Allodi, L., & Zannone, N. (2021). Dissecting social engineering attacks through the lenses of cognition. 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) ,

Bustio-Martínez, L ,.Herrera-Semenets, V., García-Mendoza, J. L., Álvarez-Carmona, M. Á., González-Ordiano, J. Á., Zúñiga-Morales, L., Quiróz-Ibarra, J. E., Santander-Molina, P. A., & van den Berg, J. (2024). Uncovering phishing attacks using principles of persuasion analysis. *Journal of Network and Computer Applications*, *230*, 103964 .

Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. (2016). Breaching the human firewall: Social engineering in phishing and spear-phishing emails. *arXiv preprint arXiv:1606.00887* .

Chapagain, D., Kshetri, N., Aryal, B., & Dhakal, B. (2024). SEAtech: Deception Techniques in Social Engineering Attacks: An Analysis of Emerging Trends and Countermeasures. *arXiv preprint arXiv:2408.02092* .

Chen, D. Q., Preston, D. S., & Xia, W. (2010). Antecedents and effects of CIO supply-side and demand-side leadership: A staged maturity model. *Journal of Management Information Systems*, *27*(1), 231-272 .

Gámez-Guadix, M., Almendros, C., Calvete, E., & De Santisteban, P. (2018). Persuasion strategies and sexual solicitations and interactions in online sexual grooming of adolescents: Modeling direct and indirect pathways. *Journal of Adolescence*, *63*, 11-18 .

Greavu-Serban, V., & Serban, O. (2014). Social engineering a general approach. *Informatica Economica* .5 ,(2)18 ,

Hadnagy, C. (2010). *Social engineering: The art of human hacking*. John Wiley & Sons .

Halevi, T., Lewis, J., & Memon, N. (2013). A pilot study of cyber security and privacy related behavior and personality traits. Proceedings of the 22nd international conference on world wide web ,

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, *50*(10), 94-100 .

Jones, K. S., Armstrong, M. E., Tornblad, M. K., & Siami Namin, A. (2021). How social engineers use persuasion principles during vishing attacks. *Information & Computer Security*, *29*(2), 314-331 .

Junger, M., Koning, L., Hartel, P., & Veldkamp, B. (2023). In their own words: deception detection by victims and near victims of fraud. *Frontiers in psychology*, *14*, 1135369 .

Kaptein, M., De Ruyter, B., Markopoulos, P., & Aarts, E. (2012). Adaptive persuasive systems: a study of tailored persuasive text messages to reduce snacking. *ACM Transactions on Interactive Intelligent Systems (TiiS)*, *2* .25-1 ,(2)

Khadka, K. (2024). Persuasion and Phishing: Analysing the Interplay of Persuasion Tactics in Cyber Threats. *arXiv preprint arXiv:2412.18485* .

Khadka, K., Ullah, A. B., Ma, W., Marroquin, E. M., & Alem, Y. (2023). A survey on the principles of persuasion as a social engineering strategy in phishing. 2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) ,

Koddebusch, M. (2022). Exposing the phish: the effect of persuasion techniques in phishing e-mails. Proceedings of the 23rd Annual International Conference on Digital Government Research ,

Mangoud, & Ali, H. M. M. (2022). Planning to raise university youth awareness of the dangers of cybercrime. *Studies in Social Service*, *60*(2), 379-418 .

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

Montañez, R., Golob, E., & Xu, S. (2020). Human cognition through the lens of social engineering cyberattacks. *Frontiers in psychology*, *11*, 1755 .

Pasricha, P., & Mehrotra, S. (2014). Electronic crime in Indian banking. *Sai Om Journal of Commerce and Management*, *1*(11), 7-14 .

Qwaisy, M. R., & Alhalwany, H. A. (2024). The electronic fraud among rural university youth A field study on students of Agriculture Faculty, Al-Azhar University, Assiut. *Fayoum Journal of Agricultural Research and Development*, *38*(4), 476-502 .

Rajivan, P., & Gonzalez, C. (2018). Creative persuasion: a study on adversarial behaviors and strategies in phishing attacks. *Frontiers in psychology*, *9*, 135 .

Rao, H. S. (2019). Cyber crime in banking sector. *International Journal of Research-Granthaalayah*, *7*(1), 148-161 .

Ryder, N., & Reid, A. S. (2012). E-Crime. In (Vol. 21, pp. 203-206): Taylor & Francis.

Sabillon, R ,.Cano, J. J., & Serra-Ruiz, J. (2016). Cybercrime and cybercriminals: A comprehensive study. *International Journal of Computer Networks and Communications Security, 2016, 4* .(6)

Schmitt, M., & Flechais, I. (2024). Digital deception: Generative artificial intelligence in social engineering and phishing. *Artificial Intelligence Review*, *57*(12), 1-23 .

Sherman, M. (2000). *Introduction to cyber crime*. Federal Judicial Center .

Siddiqi, M. A., Pak, W., & Siddiqi, M. A. (2022). A study on the psychology of social engineering-based cyberattacks and existing countermeasures. *Applied Sciences*, *12*(12), 6042 .

Van Der Zee, S., Clayton, R., & Anderson, R. (2019). The gift of the gab: Are rental scammers skilled at the art of persuasion? *arXiv preprint arXiv:1911.08* .253

Wang, Z., Sun, L., & Zhu, H. (2020). Defining social engineering in cybersecurity. *IEEE access*, *8*, 85094-85115 .

Wang, Z., Zhu, H., & Sun, L. (2021). Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. *IEEE access*, *9*, 11895-11910 .

Wantenaar, L. (2022). Social engineering and the use of persuasion to commit cyber fraud. *Cyber Security: A Peer-Reviewed Journal*, *6*(2), 102-110 .

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American society for information science and technology*, *59*(4), 662-674 .

Wright, R. T., & Marett, K. (2010). The influence of experiential and dispositional factors in phishing :An empirical investigation of the deceived. *Journal of Management Information Systems*, *27*(1), 273-303 .

Yar, M. (2012). E-Crime 2.0: The criminological landscape of new social media. *Information & Communications Technology Law*, *21*(3), 207-219 .

Zhang, Y ,.Xiao, Y., Ghaboosi, K., Zhang, J., & Deng, H. (2012). A survey of cyber crimes. *Security and Communication Networks*, *5*(4), 422-437 .