SOCIAL ENGINEERING AND DIGITAL FRAUD: STUDYING THE DIFFERENCES BETWEEN VICTIMS OF CYBER PHISHING IN LIGHT OF SOME VARIABLES

Shaden Ali AbdullahAl-Nafisa[1], Prof. Yahya MKhatatbeh[2]

[1,2]Imam Mohammad Ibn Saud Islamic University (IMSIU), KSA.

[1]444011427@sm.imamu.edu.sa
[2]ymkattabh@imamu.edu.sa

Corresponding ymkattabh@imamu.edu.sa

ABSTRACT

Objective: This study aimed to reveal differences in the levels of exposure to social engineering among victims of cyber deception, in light of a number of demographic variables, including: gender, age, educational stage, and educational level. The study relied on the descriptive analytical approach, being the most appropriate for the nature of the problem and the objectives of statistical analysis of differences. Method: The study sample consisted of (164) male and female students (77 males,87 females) who were selected by a simple random sample method from the student community of the College of Science and Arts, the study sample consisted of (164) male and female students who are victims of electronic deception, they were selected using a simple random sample. The study used the scale of social engineering (Abdel Tawab, 2021). Results: The results showed that there were no statistically significant differences in the socio-technical engineering dimension according to the gender variable or the most commonly used electronic application variable. On the other hand, significant differences appeared in the dimension of human social engineering and the overall scale in favor of older students (26 years and over) and diploma students. Meta-analyses also showed that the age group (18–25) recorded lower levels of exposure to cyber deception, and the results revealed that the age, educational level and most commonly used application had statistically significant effects on exposure to social engineering, particularly in human-based tactics and on the public domain. In contrast, sex showed little effect. These findings highlight the importance of targeting specific demographic groups in outreach programs to promote digital safety among university students. Recommendations: The study recommends designing awareness programs targeting the most vulnerable groups, especially diploma students and older students, and integrating digital security concepts into university curricula.

Keywords: social engineering, phishing,phishing victims.

INTREDECION

With the acceleration of digital transformation and the spread of electronic services, cyber threats, especially those based on social engineering, one of the most sophisticated and deceptive fraud technologies, have become more serious.This type of fraud is not based on hacking systems, but rather on exploiting the psychological and social nature of the individual to access his data, money or sensitive information. (Hadnagy & Fincher, 2018). Cybersecurity reports indicate that more than 85% Some data breaches are due to reasons related to user behavior, especially their response to phishing and impersonation. (Verizon, 2023). Social engineering is one of the most prominent means used in this, and its methods vary between fraudulent phone calls, misleading text messages, and fake websites that mimic official sites. (Mouton et al., 2016)، Multiple studies have shown that the victims of these attacks are not only elderly or uneducated, but also include young and highly educated groups, indicating the complexity of the phenomenon and the intertwining of its variables. (Jagatic et al., 2007; Sheng et al., 2010), and in In this context, it is noted that digital security awareness plays an important role in predicting the individual's victimization of these fraudulent practices. (Arachchilage & Love, 2014)Differences between victims vary according to demographic, personality and behavioral variables; for example, the literature suggests that people with a high tendency to trust others or who have a weakness in critical thinking are more likely to respond to fraud attacks.(Wright & Marett, 2010) Personality traits such as extroversion and openness may also be associated with higher levels of exposure to cyber scams.(McCormac et al., 2017), stands out The importance of analyzing the differences between victims of digital fraud in light of a set of variables, in order to reach a deeper understanding of the factors that increase individuals' vulnerability to targeting.

This study is based on the theory of planned behavior(Ajzen, 1991)From a humanitarian perspective, the effects of this phenomenon are not limited to physical aspects, but extend to psychological dimensions such as anxiety, loss of trust in others, and exposure to social stigma, especially in cases where the victim is from a vulnerable group such as women or adolescents. (Button et al., 2013; Cross et al., 2016) Some studies suggest that the psychological response after fraud may last months or years, which reinforces the need for both preventive and curative intervention. (Buchanan & Whitty, 2014) Hence the importance of this study, which aims to analyze the differences between victims of electronic deception based on a number of variables, in an attempt to understand the nature and methods of targeting, propose ways to prevent and build awareness programs based on realistic and in-depth analysis.

Confirmed (Siddiqi et al., 2022)moan Attacks Social Engineering Exploit Certain human traits and psychology to bypass technical security measures, making them effective methods and hidden in Penetrating any organization.In this context, Understanding tactics These attacks are an essential step to prevent them, and in the study of(Banire et al., 2021) find That of more prominent The reasons Exposure of victims to attack is lack of focus and ignorance of attack methods, and many Internet users have difficulty recognizing deception methods, similar to those that occur in direct offline contact. (Norris et al., 2019)A study has shown (Junger et al., 2023)40% of victims believe that The attack could have been avoided if they had researched further or followed more precise security measures.

as carry out (Collier & Morton, 2024)A study in the United States of America aims to analyze the behavior of adolescents when using social media, their interaction with the algorithms used in electronic applications, and analyze how social media platforms contribute to facilitating social engineering. The most prominent results indicated that Social media platforms are an influential factor in the occurrence of social engineering, through the influence of algorithms on user interaction and behavior by providing targeted content that enhances the tendency to reduce verification From social engineering methods, Like algorithms and interaction mechanisms, they play an important role in enhancing users' exposure to social engineering. The results showed that adolescents' acceptance of virtual relationships with unknown people increases their likelihood of exposure to the risks of social engineering. (Parti, 2023)A study aimed at comparing the characteristics of victims of electronic deception aged between (18-55) years, and victims aged (55) years and over, according to the theory of routine activity The study sample consisted of (2589) citizens, aged (18) years and over. The most prominent results indicated a statistically significant relationship between computer use at work and falling victim to all types of electronic deception. Younger individuals with computer-related professional routines were significantly more likely to fall victim to deception than older individuals. The results also revealed that single parents were less likely to be deceived than those living with a partner or children. In contrast, older people who work full-time were more likely to fall victim to cyber fraud than retirees, especially with regard to corporate impersonation deception. The study also aimed at (Almutairi & Alghamdi, 2022)into measurement Level of engineering awareness Social and Presentation Suitable solutions to reduce their risks. The questionnaire was applied to (508) Participants From different organizations in Riyadh, Saudi Arabia, where the sample included employees, students, and individuals from other professions. The results showed that (63.4%) of the sample have no idea about social engineering, and (67.3%) is not They have any Knowledge of its threats، While (42.1٪) own poor knowledge, and(7.5%) Only they have a good knowledge of social engineering. The results also showed that the age group (26-35 years) and those over (45 years) are the most at risk, while the age group (18-25 years) is the most aware of the concept of social engineering. The study also indicated that females are more aware of this concept than males, and that two-thirds of respondents need to attend training courses on social engineering. (Zhang & Ye, 2022) to know the social and psychological factors associated with individuals becoming victims of cyber phishing in China. The electronic questionnaire was applied to (504) victims of electronic deception, aged between (31-89) years, in addition to (523) people who were not subjected to electronic deception, aged between (39-46) years, and the results indicated that the victims were more impulsive, more inclined to trust, and more frequent, to use smartphones compared to non-victims. They were also exposed to negative life events at a higher rate and received less social support. In contrast, there was little effect of sex on the likelihood of falling victim to cyber deception. The results also showed that younger, less educated individuals were significantly more likely to be cyber-phished than others.

Recent research highlights the evolving complexity of social engineering and phishing methods driven by AI advancements. manifest(Weinz et al., 2025) Both phishing emails generated by Quishing The LLM has resulted in high engagement rates, with more than 30٪ From clicks in some organizations. define(Schmitt & Flechais, 2024)Three transformative vectors through which generative AI enhances social engineering: Realism, customization and automation, similarly, found (Khadka, 2024) Persuasive methods such as distraction and authority dominate phishing content structures, as shown(Francia et al., 2024)Using the framework TRAPD, that phishing messages generated by WHY They were considered more convincing than those written by humans and in support of these trends, the report KnowBe4 Year 2025 Increase by 22.6% In AI-enhanced phishing with AI-enhanced ransomware, showing 92% of threats polymorphic behavior (KnowBe4, 2025)

Given the increasing sophistication of digital fraud techniques, particularly those using psychological manipulation and generative artificial intelligence, the current study addresses a fundamental and necessary research gap. By examining the disparity in vulnerability to social engineering across key demographic, cognitive, and behavioral variables, this research aims to clarify vulnerability patterns often overlooked in technical cybersecurity models. The multidimensional study framework integrates psychological theory, risk exposure measures, and experimental threat analysis, providing a holistic perspective on why some individuals fall victim to digital deception. Ultimately, the results are expected to enrich targeted prevention strategies and awareness programs, contributing to the promotion of digital citizenship in an era of rapidly evolving cyber threats.

Hypotheses

H1There are statistically significant differences in the rate of social engineering occurrence among phishing victims based on (gender, age, or educational level, the most frequently used application)

H1There are statistically significant effects of demographic variables (gender, age, education level, and most used application) on the level of exposure to social engineering among victims of electronic fraud.

MATERIALS AND METHODS

Participants

The study relied on the descriptive analytical approach as the most appropriate for the nature of the research objectives, which aims to analyze the differences in the levels of exposure to social engineering among victims of electronic deception. The study sample was selected using a simple random sample methodology from a population consisting of all students officially enrolled in the College of Science and Arts in one of the public universities, which numbered (4807) male and female students according to the statistics of 2024.The sample size was (164) male and female students who had previously been subjected to electronic deception attempts, and they were selected according to specific conditions, including: that the student be officially registered in the college during the second semester of the academic year 2024-2025, and be 18 years old or over, and voluntarily agree to participate in the study after being informed of its purpose. The graph shows the demographic distribution of the study sample, where undergraduate students constituted (76.2%) of the total sample, compared to (23.8%) of diploma students. The sample was distributed in terms of sex to (46.9%) males and ** (53.1%) females**. This distribution shows a relative equilibrium that supports the representation of the indigenous community and enhances the validity of the results for statistical analysis and general conclusion.

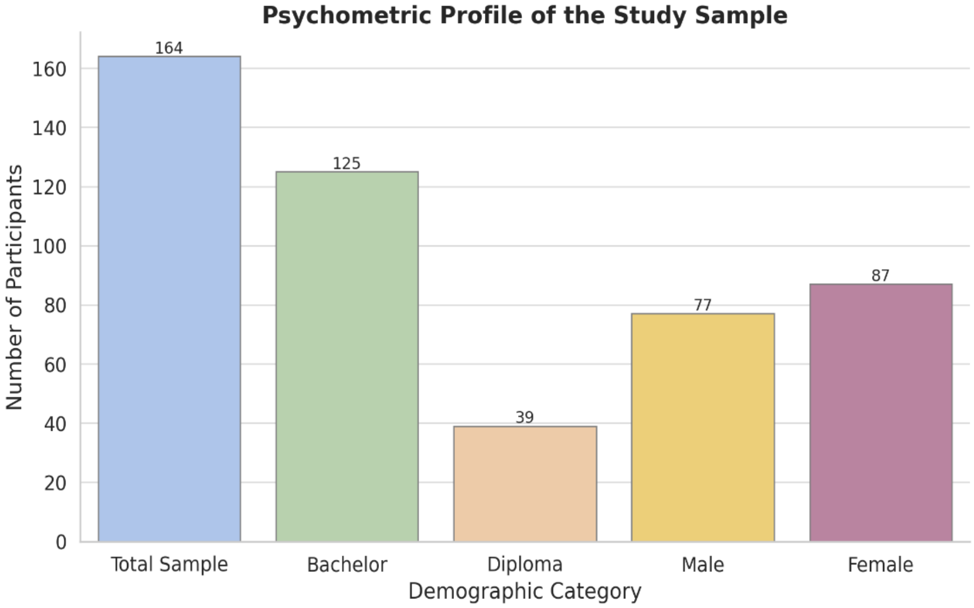


Figure 1. Demographic Profile of the Study Sample by Gender and Educational Level

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. The correlational validity of the scale was verified by calculating the correlation coefficients between each paragraph and the dimension to which it belonged, as well as between the paragraphs and the overall scale.. The correlation coefficients between the paragraphs and their sub-dimensions ranged between 0.53 into 0.81, all of which were statistically significant at the level of (0.01), reflecting significant consistency between the components of the scale. The correlation coefficients between the two dimensions and the overall scale also showed a high correlation, with the correlation coefficient of the socio-technical engineering dimension (t = 0.79), and for the human dimension (t = 0.84), indicating the construction sincerity of the scale. In terms of stability, it was verified using two methods.: First of all: Cronbach alpha coefficient for measuring internal consistency, which has reached for the scale as a whole (0.905), and reached the technical dimension (0.882), and for the human dimension (0.891), which are elevated values indicating a high degree of internal consistency. secondly: Re-application method (test-retest), where the scale was applied to an exploratory sample consisting of (30) male and female students with an interval of two weeks, and the results showed a stability coefficient of (0.87) for the overall scale, confirming the stability of the instrument over time.

RESULTS

1. **Differences in social engineering averages amongvictims of cyber deception according to the gender variable**

The graph shows slight differences in levels of social engineering between males and females across the three dimensions: technical, human, and grand total, and in the technical dimension, females scored a higher average (34.70) compared to males (34.17), with less dispersion in responses. Similarly, in the human dimension, females narrowly excelled (33.89 versus 33.43). On the overall scale, females averaged (68.59) and was higher than males (67.60). Despite these differences, the results of the T test indicate that it is not statistically significant, which means that there is no significant difference between the sexes in the level of exposure to social engineering.

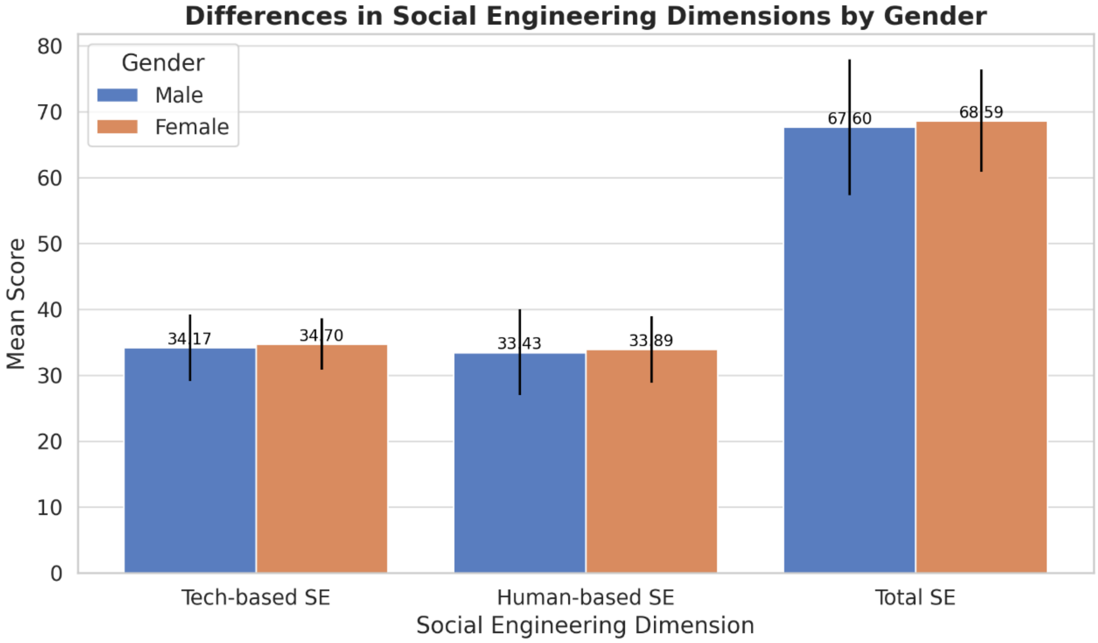


Figure2. Mean differences in social engineering dimensions by gend*er*

2. **Differences in social engineering averages among victims of cyber phishing according to the age variable**

Figure 2 shows the results of the Single Variance Test (ANOVA) to examine differences between groups in exposure levels to social engineering dimensions. The results show that the socio-technical engineering dimension did not record statistically significant differences between groups (p = 0.083), while significant differences appeared in the human social engineering dimension (p = 0.028) and in the overall scale of social engineering (p = 0.020), indicating a significant effect of some of the studied variables on these two dimensions. F-values highlight the difference in the explanatory power of each dimension, and the colors show the significance of statistical results

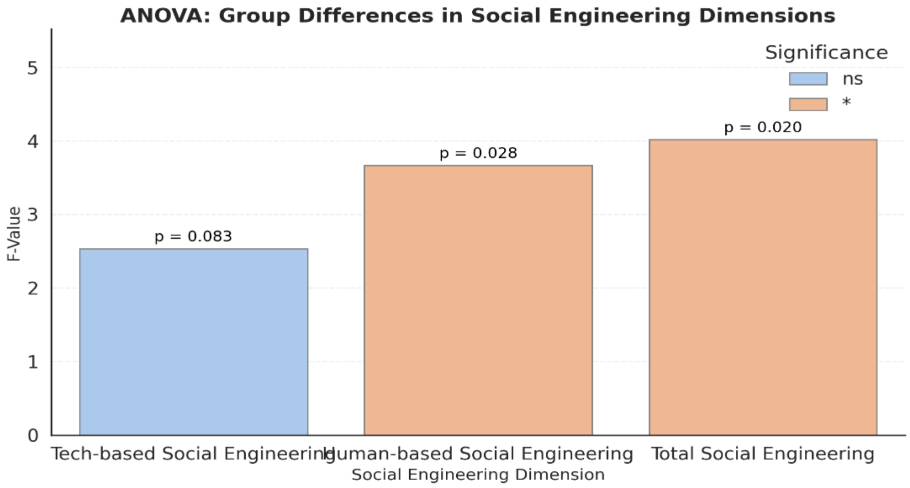


Figure3. One-way ANOVA results showing group differences across social engineering dimensions

To determine the validity of the differences between each two age groups towards the trend around these dimensions, the "LSD" test was used , and these results are shown in the following figure:

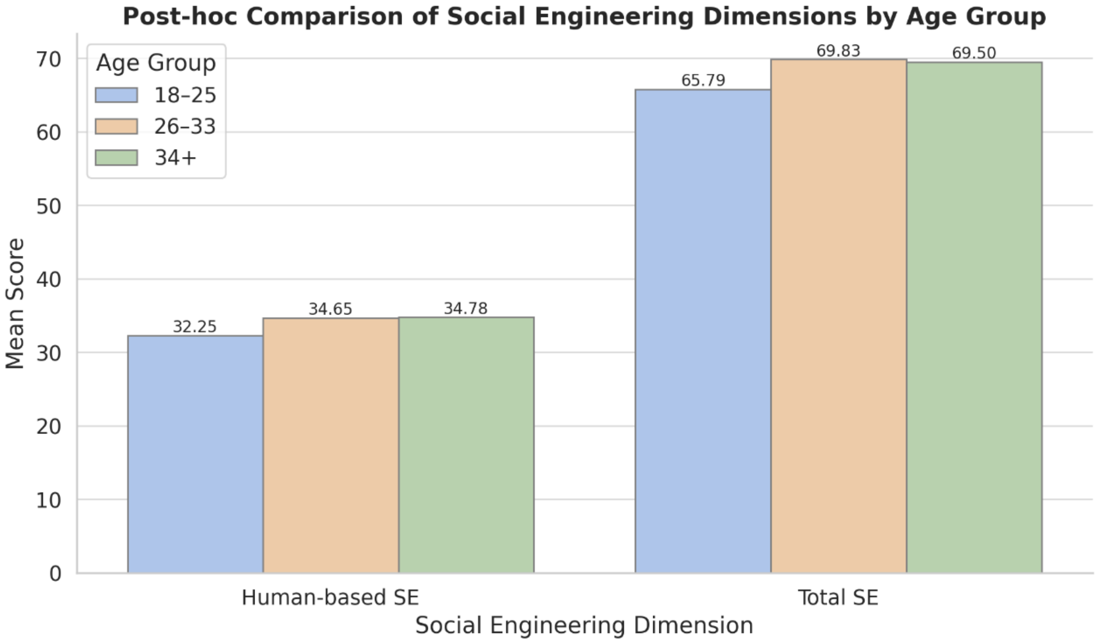


Figure4. Post-hoc comparison of social engineering exposure across age groups, **.**highlighting mean differences in human-based and total scores

This Figure shows the results of post-hoc analysis of the differences between age groups in two dimensions of social engineering: In the human social engineering dimension, the 18–25 years old group shows the lowest average (32.25), compared to the 26–33 years and34 years and over groups (34.65 and 34.78 respectively)., which indicates that the older groups are more exposed to this type of deception, and in the overall scale of social engineering, the younger group also recorded a lower average (65.79) compared to the older groups (about 69.5 or more), with a clear statistical significance, and the drawing highlights the differences in an easy visual way, and clearly shows the superiority of older age groups in the average exposure to social engineering

3. Differences in social engineering averages among victims of cyber deception according to the study trip variable

The results of the (t-test) indicate that there are no statistically significant differences between diploma students and undergraduate students in the socio-technical engineering dimension (p = 0.243), which indicates the convergence of their levels of exposure to this type of digital deception, and in contrast, the results showed statistically significant differences in the dimension of human social engineering (t = 2.256, p = 0.025), where diploma students scored a higher average (35.46). compared to undergraduate students (33.11), reflecting a variation in response to methods that rely on human manipulation, and statistically significant differences were recorded in the overall scale of social engineering (t = 2.015, p = 0.046), indicating that diploma students are generally more susceptible or engaged to social engineering practices than their undergraduate counterparts

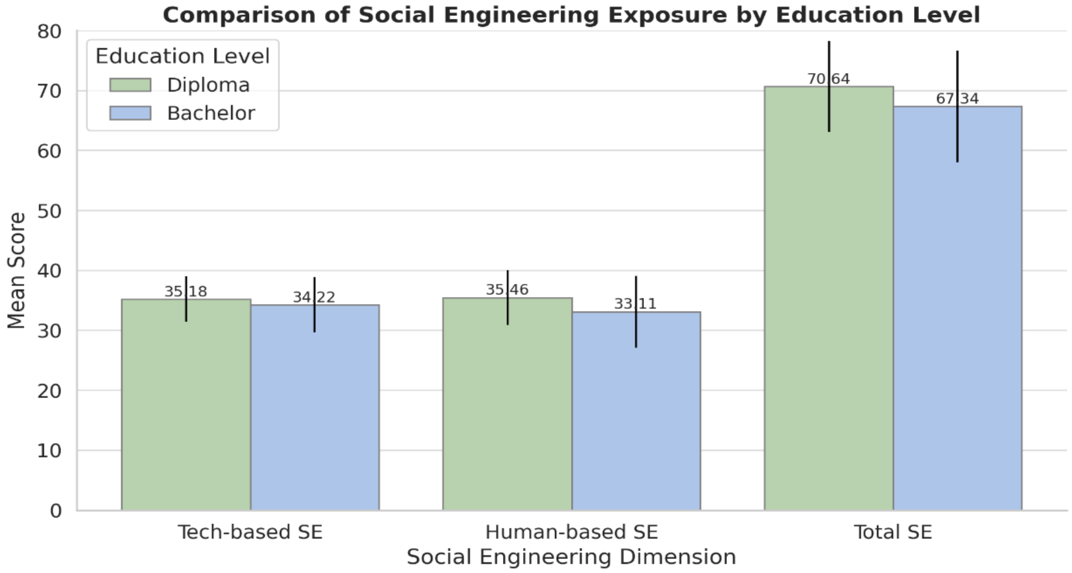


Figure5. Differences in social engineering dimensions between diploma and bachelor students, including standard deviations.

4. Differences in social engineering averages among phishing victims according to the most commonly used application variable

The results of the analysis of single variance indicate that there are no statistically significant differences between the different groups in any of the dimensions of social engineering, in the technical dimension, the value of (F = 0.676, p = 0.669), which is not significant, and in the human dimension, the value of (F = 1.047, p = 0.397), which also indicates the absence of statistically significant differences between groups, as for the total scale of social engineering, the value was (F = 0.647, p = 0.692), which is the highest in significance (p-value), and conclusively indicates that there is no significant effect attributed to the source of variation used (such as the variable of specialization or educational background), and accordingly, the results show that different groups are similar in their level of exposure to social engineering in all its dimensions, according to the variable used in this analysis.

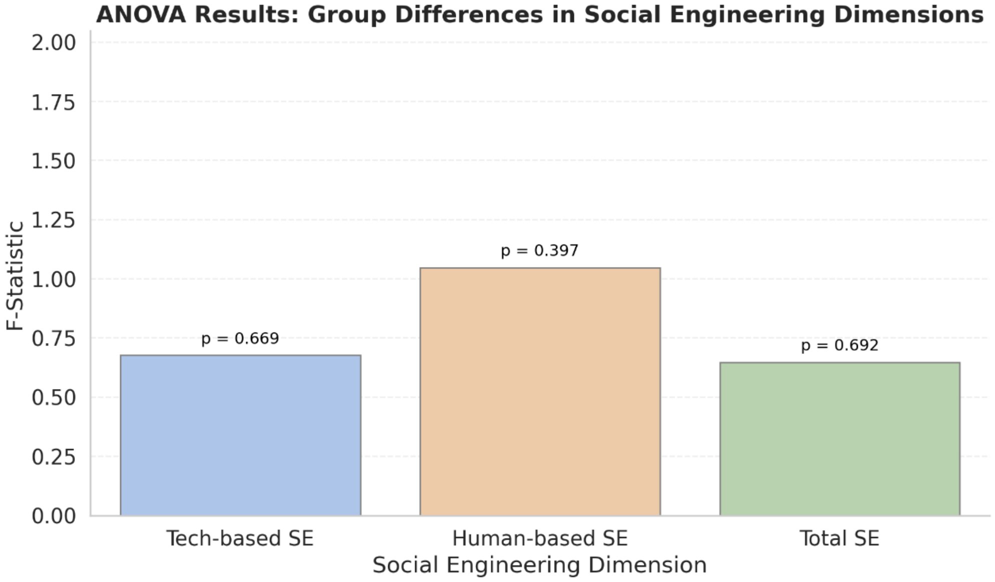
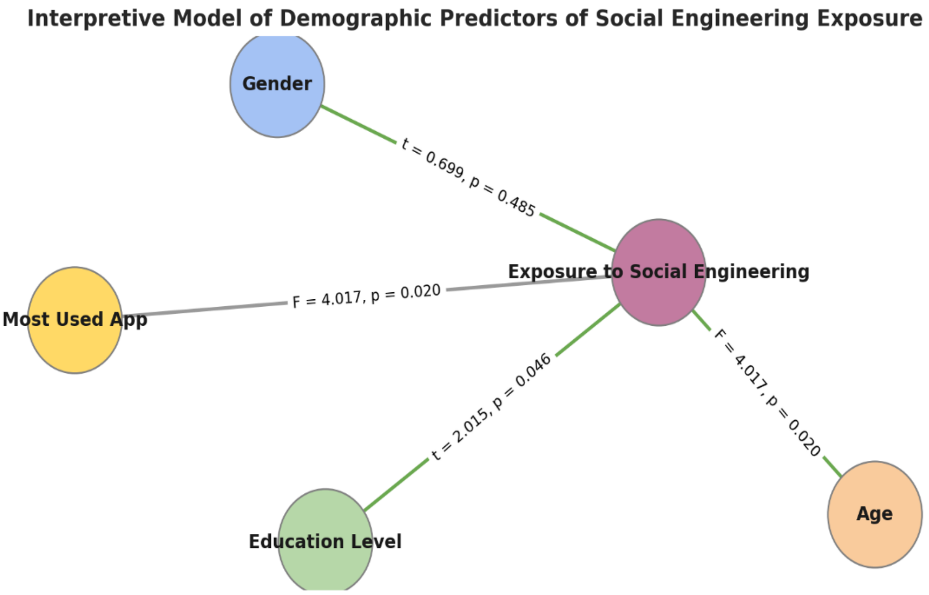


Figure6. ANOVA results for group differences in social engineering dimensions with non-significant outcomes (p > 0.05 for all dimensions)**.**

5. The effect of demographic variables (gender, age, educational level, most commonly used application) on the level of exposure to social engineering among victims of cyber deception.

This explanatory model illustrates the relationship between a set of demographic variables and the level of exposure to social engineering among university students, based on the results of the statistical analysis of the study. Age, educational stage, and the type of application most used showed a statistically significant effect on the level of exposure, with p-values less than 0.05, indicating that these variables contribute significantly to explaining the participants' varying responses to electronic deception methods, and in contrast, the gender variable did not have a significant effect, which means that males and females are relatively equal in their pattern of exposure to social engineering within the studied sample, and the model reflects in an interactive visual way the importance of behavioral and technical variables. At the expense of fixed personality traits, it provides a scientific basis for directing e-awareness programs towards the most at-risk groups.



"**Figure**7: Interpretive Model of the Impact of Demographic Variables on Social Engineering Exposure among Victims of Electronic Fraud"

Discussion

The results of the current study showed that there were no statistically significant differences at the level of statistical significance (0.05) or less in the incidence of social engineering among victims of cyber deception according to the gender variable, however, this result differs from the study of(Almutairi & Alghamdi, 2022)which indicated that females are more aware than males,

The results of the study showed that there were no statistically significant differences in the rate of exposure to social engineering among victims of cyber deception according to the gender variable. This finding contradicts the findings of a study(Almutairi & Alghamdi, 2022)**,** which noted that females are more aware of the dangers of social engineering than males. This variance is explained in the light of the theory of planned behavior **(**(Ajzen, 1991)which believes that decision-making depends on cognitive and behavioral factors common to the sexes, such as perception and perceived behavioral control, which may explain why males and females are equally deceived when conditions and pressures are equal.. As for the age variable, the results revealed that there were statistically significant differences in the dimension of human social engineering and the overall scale, and the age group was (26–33 year) are the most exposed. This finding is consistent with the study of(Almutairi & Alghamdi, 2022)which clarified that the category between (26–35 year) And who are above (45) They are the most susceptible to deception. It also supported the study of(Putri, 2018)moan Younger individuals may be more aware due to the constant handling of the technique. This is explained depending on the theory of information processing(Atkinson, 1968)**,** as individuals at the age of 26–33 They often face challenges related to the balance of professional and academic responsibilities, which may reduce their attention to security details. As Erickson's psychosocial development theory points out(Newman & Newman, 1975)indicates that this category is going through a stage "Productivity vs. recession", where the individual seeks to assert himself socially, which increases the likelihood of being subjected to psychological manipulation associated with human social engineering. As for the school stage variable, the results showed that diploma students are more exposed to human social engineering compared to undergraduate students, with statistically significant differences in the overall scale as well..This is likely explained by the fact that diploma students are often less trained in dealing with digital phishing content, and may lack the analytical or contextual skills associated with evaluating emails..The educational environment may also influence the perception of digital risks, as studies such as (Zhang & Ye, 2022)Less educated individuals were more likely to be deceived by poor social and cognitive support.

As for the most commonly used electronic application variable, the results did not show statistically significant differences.This result differs with the results of the (Collier & Morton, 2024)which She explained that social media platforms represent a catalyst for social engineering through algorithms that weaken users' self-censorship.. This discrepancy can be explained by the fact that users interact with social engineering regardless of the type of application, the lesson is the method of interacting with suspicious messages or links, not the type of platform, which supports what he mentioned (Siddiqi et al., 2022)that the psychological characteristics of users are more important than technical tools in explaining the susceptibility to falling into the trap.

Finally, the explanatory model in the study showed that age, school stage, and type of application were indicative variables in explaining the disparity in exposure to social engineering, while gender had no significant effect. This finding supports its findings. (Zhang & Ye, 2022)that Psychological and demographic characteristics remain decisive factors in predicting victims of deception. This is also reinforced by the theory of cognitive biases.(Tversky & Kahneman, 1990)which suggests that overconfidence bias and cognitive fixation may make some groups more targetable, regardless of gender.

Recommendations& Limitation

Although the study provided important results that contribute to understanding the relationship between the variables studied, there are a number of limits that should be taken into account when interpreting the results. First, the study was limited to a specific sample of a particular age and geographic group, which may limit the possibility of generalizing the results to wider communities with different cultural or social characteristics. The reliance of measurement tools on subjective questionnaires may expose results to biases in response resulting from a desire to present a positive or socially acceptable image. In addition, the study followed only a quantitative approach, preventing the exploration of profound individual experiments that may contribute to enriching the theoretical and practical understanding of the phenomenon under study. The study also did not address intermediate or modified variables that may play a role in explaining the nature of the relationship between independent and dependent variables, leaving room for more in-depth analysis in this aspect. Based on the above, the study recommends conducting future research that adopts qualitative or mixed approaches, with the aim of deepening understanding about participants' experiences and their psychosocial contexts. It is also proposed to expand the sample to include populations diverse in terms of age, sex and geographical location, to ensure the validity of the generalization. In the future, it is also useful to include intermediate or modified variables in statistical models, which will help reveal the precise explanatory mechanisms behind the relationships explored in this study.

Conclusion

This study highlighted dangerous dimensions of social engineering as a hidden form of digital fraud, which goes beyond technical aspects to target the human himself. The results revealed significant differences in exposure to cyber deception based on age and school stage, with no gender effect and the type of application used, confirming that the vulnerability to becoming a victim is associated with psychological and behavioral factors rather than purely technical.These findings are important in supporting the design of targeted awareness programs for the most vulnerable, and enhancing cybersecurity from a human perspective. This study paves the way for deeper research based on understanding humans, not machines, in the face of digital threats that are evolving at an unprecedented pace.

Finding statement

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

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.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179-211.

Almutairi, B. S., & Alghamdi, A. (2022). The Role of Social Engineering in Cybersecurity and Its Impact. *Journal of Information Security*, *13*(4), 363-379.

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304-312.

Atkinson, R. C. (1968). A proposed system and its control processes. *The Psychology of Learning and Motivation*, *2*.

Banire, B., Al Thani, D., & Yang, Y. (2021). Investigating the experience of social engineering victims: Exploratory and user testing study. *Electronics*, *10*(21), 2709.

Buchanan, T., & Whitty, M. T. (2014). The online dating romance scam: causes and consequences of victimhood. *Psychology, Crime & Law*, *20*(3), 261-283.

Button, M., Tapley, J., & Lewis, C. (2013). The 'fraud justice network'and the infrastructure of support for individual fraud victims in England and Wales. *Criminology & Criminal Justice*, *13*(1), 37-61.

Collier, H., & Morton, C. (2024). Teenagers: A Social Media Threat Vector. 19th International Conference on Cyber Warfare and Security: ICCWS 2024,

Cross, C., Richards, K., & Smith, R. G. (2016). The reporting experiences and support needs of victims of online fraud. *Trends and issues in crime and criminal justice*(518), 1-14.

Francia, J., Hansen, D., Schooley, B., Taylor, M., Murray, S., & Snow, G. (2024). Assessing AI vs human-authored spear phishing sms attacks: An empirical study using the trapd method. *arXiv preprint arXiv:2406.13049*.

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

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.

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

KnowBe4. (2025). *Phishing threat trends r*

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, *69*, 151-156.

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security*, *59*, 186-209.

Newman, B. M., & Newman, P. R. (1975). *Development through life: A psychosocial approach*. Dorsey.

Norris, G., Brookes, A., & Dowell, D. (2019). The psychology of internet fraud victimisation: A systematic review. *Journal of Police and Criminal Psychology*, *34*, 231-245.

Parti, K. (2023). What is a capable guardian to older fraud victims? Comparison of younger and older victims' characteristics of online fraud utilizing routine activity theory. *Frontiers in psychology*, *14*, 1118741.

Putri, D. A. W. (2018). Threat Language: Cognitive Exploitation in Social Engineering.

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

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. Proceedings of the SIGCHI conference on human factors in computing systems,

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.

Tversky, A., & Kahneman, D. (1990). Judgment under uncertainty: Heuristics and biases.

Weinz, M., Zannone, N., Allodi, L., & Apruzzese, G. (2025). The Impact of Emerging Phishing Threats: Assessing Quishing and LLM-generated Phishing Emails against Organizations. *arXiv preprint arXiv:2505.12104*.

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.

Zhang, Z., & Ye, Z. (2022). The role of social-psychological factors of victimity on victimization of online fraud in China. *Frontiers in psychology*, *13*, 1030670.