Journal of Ecohumanism
2024
Volume: 3, No: 7, pp. 2580 – 2592
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i7.4662

Awareness of Social Engineering Attacks and their Relation to the Ability to Persuade among users of Social Networking Sites

Alotayan, Turki, M[1]

Abstract

Aimed Education Current into Detection levels Awareness of social engineering attacks(ASEA) and their relationship to the ability to persuade users of social networking sites, and recognize the differences in In the level of awareness of social engineering attacks And the ability to persuade among social media users according to variables of age, place of residence, economic level, educational level, and the degree to which awareness of social engineering attacks affects the ability to mask by revealing the affective relationship between variables. The study sample consisted of (415) responding to the study tools. To achieve the objectives of the study, the social engineering scale was used by Vrhovec (2021). And the measure of persuasion ability by Busch et al. (2013. The results demonstrated that social media users' awareness of social engineering attacks and their ability to persuade were around average, with an overall scale average of 3.23 and an overall persuasion ability measure of 3.34. A correlation coefficient of 0.418 at the statistical significance level (a = 0.05) showed that there was a positive and statistically significant relationship between the participants' perceptions of their awareness of social engineering attacks and their ability to persuade on social networking sites. The results of the study also showed a statistically significant effect at the level of significance (a≤0.05) for the impact of awareness of social engineering attacks on the ability to persuade from the point of view of the study sample, as the correlation coefficient (R) (418), while the coefficient of determination (R2) indicates that awareness of social engineering attacks (as an independent variable) explains (17.5%) of the variation in the variable (ability to persuade) (as a dependent variable), and the rest of the percentage means that there are other independent variables that are not mentioned in The study model - or may be due to random error, and the results of the study indicated that there are no differences in the ability to persuade users of social networking sites according to variables, place of residence, economic level, educational level, as shown in the table that there are differences according to the two age variables, where it was found that there are differences between the category of 18-20 and the category of 24 and above and in favor of the category of 18-20 on the ability to convince totally. Regardless of demographic variables such age, place of residence, socioeconomic level, or level of education, the study found that knowledge of human engineering assaults was constant.

Keywords: *Awareness of Social Engineering Attacks Persuasion Social Media Users.*

Introduction

Social engineering attacks on social media are a growing concern, exploiting human psychology to gain unauthorized access to sensitive information (Naz et al., 2024). Such attacks can lead to significant financial losses and data breaches. (Banire et al., 2021) Research suggests that social engineering awareness is critical in enhancing users' security protection practices and improving their ability to detect deceptive messages. (Alseadoon, 2023)However, hackers regularly exploit the trust of social media users for their own gains, often using phishing attacks, and phishing messages are both a scam and a trade (Chetioui et al., 2022) Phishing and identity theft are social media threats. To steal your personal information or upload dangerous stuff, attackers may spoof respectable connections or corporations.

Social engineering assaults represent growing security risks. A 2011 global survey of 853 IT experts in the US, UK, Canada, Australia, New Zealand, and Germany found that social engineering assaults are more costly in large organizations. Around 48% of major corporations and 32% of all enterprises have had 25+ social engineering attempts in the past two years. In 2018, 85% of organization's experienced social engineering attacks, a 16% increase from the previous year. Annual enterprise social engineering attacks in 2010-2018 cost 1.4 million dollars, up 8% from the preceding year. (Wang et al., 2020). Social engineering attacks have spread, especially on social media, As: Facebook & Twitter which Targeting people's emotions rather than their technological vulnerabilities, increasing user awareness is essential to achieving effective cybersecurity (Krombholz et al., 2015) where Cybercriminals find social media to be the perfect place for social engineering strategies due to the abundance of freely available information it offers (Algarni, 2019). Despite the increased danger, many social media users either don't know or don't

[1] College of Social Sciences, Department of Psychology, Imam Mohammad Ibn Saud Islamic University, Saudi Arabia (IMSIU), Riyadh; Criminal psychology - Counseling and rehabilitation. E-mail: tmotayan@imamu.edu.sa

Journal of Ecohumanism
2024
Volume: 3, No: 7, pp. 2580 – 2592
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i7.4662

believe that social engineering attacks are dangerous. For example Between (Vishwanath et al., 2018)That many social media users have had difficulty recognizing phishing efforts. Additionally, as mentioned (Salahdine & Kaabouch, 2019) Social media users who provide too much personal information risk targeted attacks.‘ Current social engineering strategies are complicated, making the knowledge gap concerning. Attackers create phone profiles and exploit trusted relationships, making it hard for users to tell good from negative interactions. (Ivaturi & Janczewski, 2019). Due to the widespread use of social media and its importance in professional and personal interactions, information security research on social engineering vulnerabilities and how to raise awareness has become important.

Awareness of Social Engineering Attacks

Social engineering attacks pose significant cybersecurity threats because they exploit human vulnerabilities rather than technical vulnerabilities. (Aldawood et al., 2020) Attacks can damage critical data and inflict major financial losses. Interactive outreach programs work better than standard training. Social engineering attacks affect national and international security beyond individual and organizational levels Akyeşilmen and Alhosban (2024), considered In the digital age, social assault engineering exploits human psychology to achieve harmful purposes, making it one of the biggest hazards to social media users. Attackers use psychology and human behaviors to persuade victims to reveal critical information or make beneficial judgements.

Social engineering awareness is the knowledge and understanding of cybercriminals' psychological manipulation methods to exploit human vulnerabilities and gain unauthorized access to sensitive data, systems, and physical areas. Understanding social engineering—an attack method that exploits human psychology, naivety, and ignorance rather than technical vulnerabilities—recognizing common social engineering tactics like phishing, deception, baiting, and stalking and recognizing potential signs of social engineering attempts like urgent language, unfamiliar senders, unsolicited attachments, and requests for information—are crucial to this awareness (Smith et al., 2013)

Social engineering is a sophisticated attack strategy that exploits human psychology rather than technical vulnerabilities (Schumacher & Frühjahrsfachgespräch, 2011). It includes various techniques to manipulate individuals into disclosing confidential information or take actions that would compromise security(Heartfield & Loukas, 2015). Emerging threats include the potential use of social bots to launch social engineering attacks, highlighting the need for proactive defensive strategies in this evolving landscape (Postnikoff & Goldberg, 2018). Social media users need continual security awareness training to combat these dangers. This training should address social media hazards beyond phishing, and users may help prevent them by being mindful about what they publish and attentive against common attack strategies (Ivaturi & Janczewski, 2011)

According to previous studies, a study published in the Journal of Human Demonstrating showed that approximately 30% of users targeted by phishing attacks (Phishing) on social media have responded in some way to attackers, demonstrating a significate awarenesses in awareness and training of this type of threat (Sheng et al., 2010). Studiedly as have shown of a small percentage Only users have prior knowledge of social engineering techniques (. Highlightingl., 2021) Highlighting the need for increased education and training, the effectiveness of social engineering attacks is influenced by message characteristics and users' persuas, Cybercriminals have exploited recent events, such as the COVID-19 pandemic, to launch social engineering attacks, underscoring the importance of understanding and responding to these threaTechnologicali, 2020). Technological advances and the widespread use of information technology have led to an increase in cybersecurity threats. Social engineering attacks are a common type of cybersecurity threat that everyone faces, several methods, such as invoking the use of artificial intelligence or phishing, are used to attack users' data, and the risk of data attacks has increased, as the use of digital technologies has become easier among users. (Abdulla et al., 2023) and you know Engineering Social is an offensive method that involves exploiting human weakness and ignorance‘ Although related technologies have existed for some time, current awareness of social engineering and its multiple forms is relatively low a; therefore, effortsre required to improve the protection of the user community. (Smith et al., 2013), and

Journal of Ecohumanism
2024
Volume: 3, No: 7, pp. 2580 – 2592
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i7.4662

it is among the most cutting-edge methods for acquiring sensitive information through unauthorized access to computer systems. Social engineers employ tactics like phishing to trick users into divulging sensitive information or giving them access to other systems; this type of cybersecurity threat relies on human error rather than technical know-how.(Alsulami et al., 2021) Success with social engineering tactics has always hinged on the target organization's security systems, tools, and current preventive measures, no matter how much progress has been made in this area. Furthermore, organizations should make sure their employees are well-versed in information security, social engineering, and the consequences of these threats and attacks. Employee training and competence in handling sensitive company information are crucial to the success of social engineering. (Algarni, 2019). It is within knock Common social engineering on social media sending spam, creating fake profiles, and phishing attempts (Algarni et al., 2017). Information shared on social media that can be exploited includes location data, job details, and personal information such as birthdays, Among the most prominent Skills that can be exploited by the user to reach Individual's system. **1.** Impersonation of employees: This is the art of inventing a scenario to convince the target to release information or do an action, and it is usually done Through email or phone, is considered a skill The most powerful and dangerous trick to get physical access to the system, which is pretending that the person is from within the company. **2.** Playing on the sympathy of users, the social engineer may pretend to be an outsider worker, **3.** use Tactics of intimidation Social workers may need to resort to stronger means: intimidation. **4.** Deception: It is an attempt to deceive people and convince them that something false is real. It may also lead to sudden decisions due to the fear of an unfortunate accident. 5. Create confusion: Another trick involves first creating a problem and then taking advantage of it. It can be as simple as turning on a fire alarm so everyone leaves the area quickly, without shutting down their computer (Hasan *et al.*, 2010).

The study conducted by Alsulami et al. (2021) into to assess social engineering awareness in Saudi Arabia's educational sector, 465 participants completed questions about social engineering. The study found that 34% of participants (158) had prior knowledge of social engineering methods, resulting in significant differences in security practices and skills. Training is crucial to increase awareness of social engineering attacks in Saudi education, according to this study.as Get up (Orgill *et al.*, 2004) The researchers claimed to be computer support department employees in a study to assess Internet users' awareness of social engineering and asked for user names, passwords, etc. The study's findings were alarming: 80 subjects gave their username and 60 their password. He also Karakasiliotis et al. (2006) Researchers gave participants 20 legal and illegitimate emails to identify in a social engineering study on email phishing. 36% of 179 informed people identified real emails and 45% illegal ones. People who detected fake emails often couldn't explain their choice .Twitchell (2006) also noted that most information curricula did not directly address social engineering, despite employee awareness and education, security, technical, and organizational reviews, and other preventive measures. The author recommends adding social engineering to these courses to better prepare students for social engineering risks.

The Bond study proved Bond et al. (2010)The use of social networks in advertising has a strong impact on customer brand loyalty, and even more so, And that social media has a significant impact on the consumer at all stages of the purchasing decision-making process by influencing his trends.

The Ability to Persuade Social Media Users

Social engineering relies on persuasion methods to manipulate victims to make them perform actions or reveal confidential information, and persuasion is a well-known technique used in many other fields, such as sales, marketing, insurance, etc.(Siddiqi *et al.*, 2022) Social engineering attacks on social media platforms, especially Facebook, are becoming more complex and effective in manipulating users. (Algarni, 2019) These attacks exploit psychological characteristics and persuasion techniques to influence behavior, with personal styles proving to be very successful. (Matz *et al.*, 2017) The usual use of social media and large social networks increases scams. Misuse of social media to spread misinformation and manipulate public opinion، While some interventions have shown promise in reducing vulnerability to social engineering, their effectiveness varies widely. (Vishwanath, 2015) The ability to predict personality traits from social media profiles enhances the possibility of targeted manipulation (Golbeck *et al.*, 2011)With increasing As social

Journal of Ecohumanism
2024
Volume: 3, No: 7, pp. 2580 – 2592
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i7.4662

media relates to everyday life, addressing these vulnerabilities and developing effective measures to address them is critical to ensuring user safety and maintaining the safety of online interactions.

Because of emotion, persuasion is split into morality (credibility), emotion, and logic (slogans). Logic is a person's emotional attachment and way of thinking to persuasively argue. There seems to be general agreement that these measurements evaluate information (information completeness, consistency, accuracy, adequacy, relevance, timeliness, and comprehensiveness) or persuasion. (Algarni, 2019) The recipient's perspective is crucial in determining whether a message is accepted or rejected, and can be altered by the medium, channel, or context. Looking at Facebook social engineering tricks and attempts may clarify. Different persuasion goals

Digital fingerprints like Facebook likes and tweets can correctly identify psychological traits.‘ We used digital fingerprints to analyse psychological persuasion's effects on people's behaviour in three field studies with over 3.5 million participants and psychologically prepared advertisements. Fatin Persuasive appeals that matched people's psychological traits increased clicks and sales. led to Posts Persuasion matched to people's openness to experience reported up to a 40% increase in clicks and up to 50% in purchases compared to non-matched or unassigned counterparts. The study showed that psychological targeting can influence the behaviour of large groups of people by designing Signals Convincing that meet their psychological needs.We explore how this strategy may improve decision-making and the hazards of manipulation and privacy. Psychological(Matz et al., 2017).

Attackers utilize numerous persuasion methods. On user feedback Various and related to provocation, trust and cordial understanding can convince, while dread can. Social network emotions are extractable. Detects essential information to distinguish bad and good persons. Has investigated emotional clues like: People react to social engineering attacks out of fear and anxiety: Trust, an emotional component that has gotten too little attention in earlier research, can be separated into two types: trust in the medium and trust in members. Users' trust in network providers and members affects the intensity of information exchange in the network. Trust often reduces risk awareness, making social engineering attacks more likely.(Albladi & Weir, 2018).

Methods of Influence A=and Persuasion Used by Social Engineers

Social engineers employ numerous psychological methods to influence consumers, including:**1.** Attackers use fear, excitement, curiosity, and haste to overwhelm critical thinking. The message "Your account will be deleted within 24 hours if you don't verify your information" uses fear and haste to get users to act quickly**. 2.** Abuse of trust: Social engineers impersonate friends, relatives, and legitimate organizations to win user confidence on social media. Fake freebies or exclusive offers can get consumers to reveal their personal information (Granger, 2001).

Once targeted, may Persuade the target (social engineer) to improve his odds. where Reciprocity, matching, adoration, scarcity, dedication, and authority can boost success. Reciprocity is offering something in return, and the target feels beholden to the applicant to make a gesture, even the tiniest one, that puts the applicant in a useful position, conformity, or social proof, is imitating others, admiring someone puts a person in the appropriate position, and people admire individuals who share their interests, attitudes, and views, so they are aware of these things' growing value and beauty, making them more appealing. And after promising or agreeing, commitment is the chance of committing to a cause or concept. People usually keep their promises, strengthening commitment (GuAdAGnO, 2013). According to Cialdini (2006) Reciprocity, commitment, consistency, social proof, authority, adoration, and scarcity are the six persuasion principles. Reciprocity dictates how kindness is returned, commitment is the desire for consistency in behavior. Social evidence, such as peer pressure, can include morality, music, and favourite foods. If the group is looking out the window, anyone who sees them will too. Admiration is merely approving those we love. Authority refers to people's tendency to obey authority.‘ Scarcity is a time-based persuasion strategy. Limited-time sales try to persuade people to buy before the price rises.

Journal of Ecohumanism
2024
Volume: 3, No: 7, pp. 2580 – 2592
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i7.4662

The study carried out by van der Kleij et al. (2023) In social engineering and disclosure of identifiable personal information, a population-based survey experiment examines the relationship and influencing factors, Where People routinely provide personally identifiable information (PII) that cybercriminals can use against them. Cybercriminals utilise persuasion to deceive people. Research suggests that reciprocity and authority can reduce persuasion, particularly when it comes to information security and positive influence. The study sample included 2426 individuals ('A = 2426). The study found that people share more personally identifiable information when urged to reciprocate, but not by authority. Information security expertise also affects disclosure. Contrary to expectations, study subjects disclosed less personally identifiable information when they knew more about information security, the positive effect was not associated with disclosure, and there were no moderate effects on persuasion and disclosure. Possible causes, limitations, and future research were discussed.

Questions

- What is the level of awareness of human engineering attacks among social media users?
- What is the level of persuasion of social media users?
- What is the relationship between awareness of human engineering attacks and the ability to persuade social media users?
- What are the differences in the level of awareness of human engineering attacks among social media users according to the variables of age, place of residence, economic level, and educational level? (Multiple Variance Analysis)
- What are the differences in the persuasion ability of social media users according to the variables of age, place of residence, economic level, and educational level?
- To what degree does awareness of human engineering attacks affect the persuasion capacity of social media users?

Methodology

Methodology: This study used the quantitative (descriptive correlational) method since it was appropriate. This method involves gathering data, answering research questions, and characterizing natural and social processes, then statistically analyzing the findings.

Limitations

The tools applied to Riyadh social networking site users to measure awareness of social engineering attacks and persuasion ability represent the study's limits, so the generalization of the study's results is related to the category in which it was conducted.

Participants

In the current study, 415 social networking site participants were randomly selected from different academic levels, with an average age of 20 years, by answering a Google Form link and meeting the study's conditions. Users of Twitter, WhatsApp, Snapchat, and Instagram who have been exposed to social engineering attacks consent to the study. Demographic characteristics included age. The study participants were 18–20 years old (39%), 20–24 years old (36%), and 25 years old (23%), all of whom had a high educational level, with 76% in the bachelor's stage and 24% in the secondary stage. Ghee was found in the north of Al-Rayas (45%), central Riyadh (30%), the south (21%), and villages (3.6%).

Journal of Ecohumanism
2024
Volume: 3, No: 7, pp. 2580 – 2592
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i7.4662

Instrument

1. **Social Engineering Scale** Prepared by Vrhovec (2021) Component From (15) Distributed throughout 45 paragraphs, Range Options Strongly agree and estimate 5 points, strongly disagree and estimate 1 point. In this study, Pearson's correlation coefficient was verified for the dimensions (perceived intensity, weakness, threat, fear, subjective base, attitude towards behaviors, behavioral control, self-efficacy, effectiveness of response, trust in responsible institutions, intended organization, official performance, information sensitivity, privacy concerns, behavioral intent).

2. **The persuasiveness scale** prepared by Busch et al. (2013) consisting of (5) dimensions distributed over (25) paragraphs, and the answer options range from strongly agree, which is estimated at 5 degrees, to strongly disagree, which is estimated at one degree. The current study verified the Pearson correlation coefficient for the study dimensions, and the dimensions were as follows (incentives and rewards, competition, social comparison, trust, social learning), and the values of the correlation coefficients ranged (532,; 695,; 814.; 443.; 765.) respectively for the correlation of the dimensions with the tool as a whole, and the Cronbach's alpha reliability for the total score reached (0.91), which are appropriate values for the current study.

Data Collection and Analysis

Data Gathering and Analysis Developing and validating study tools and sending the survey URL via Google Drive were the survey's methods. 3) After reading the first page of the test instructions, participants consented. The text also told individuals that participation was voluntary, discussed any potential benefits and dangers, and emphasized how the researchers would keep participants' data secret and anonymous. 4) SPSS v. 29 was used to enter survey data, extract, analyses, and interpret results. Multiple analysis of variance, means, standard deviations, Pearson's correlation coefficient (r), and simple regression were employed to find relationships and variable effects.

Results

Arithmetic averages of the farthest social engineering attack awareness scale among social media users.

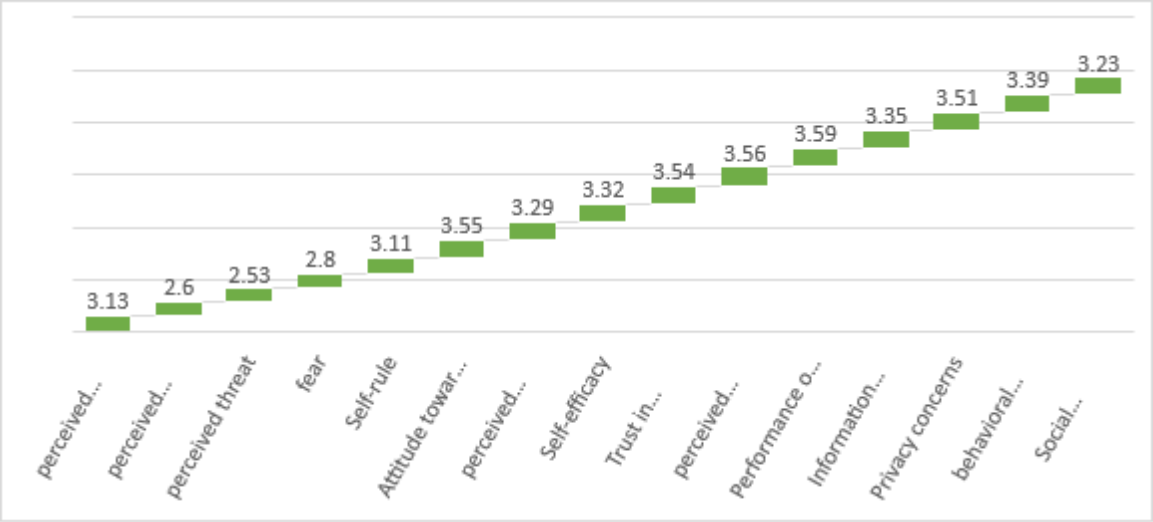

Figure (1) shows the arithmetic averages of the dimensions of the scale of awareness of social engineering attacks among users of social networking sites, as the highest of these dimensions was the official performance provided to them with an average of (3.59), while the lowest of these dimensions came the

Journal of Ecohumanism
2024
Volume: 3, No: 7, pp. 2580 – 2592
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i7.4662

perceived threat with an average of (2.60) and the total average of the scale as a whole was (3.23) with an average degree among the target study group.

Arithmetic medians of awareness levels of persuasion among social media users

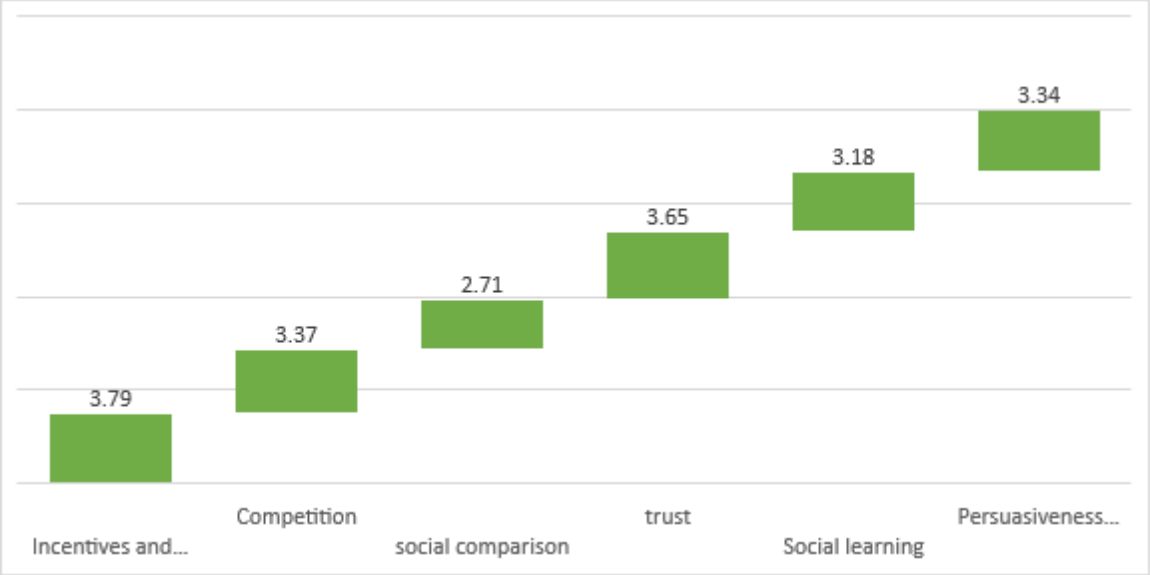

Figure (2) shows the arithmetic averages of the dimensions of the persuasion ability scale in the study group, as the highest of these dimensions was represented in the biases and rewards provided to them with an average of (3.79), while the lowest of these dimensions came social learning with an average of (3.18) and the total average of the scale as a whole was (3.34) with an average degree in the target study group.

The relationship between awareness of social engineering attacks and the ability to persuade among social media users

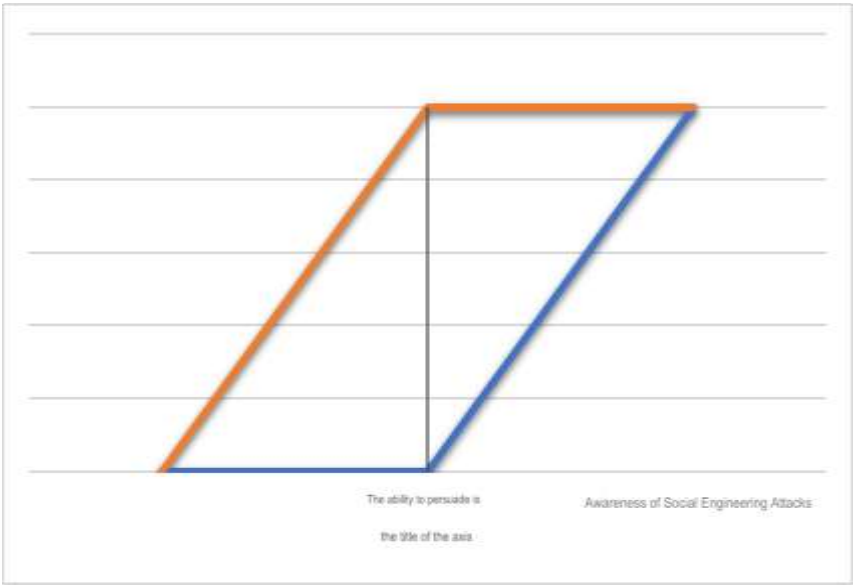

Figure (3) clear from that there is a positive relationship of statistical significance at the level of statistical significance ($\alpha = 0.05$) between the estimates of the study members between awareness of social engineering

Journal of Ecohumanism
2024
Volume: 3, No: 7, pp. 2580 – 2592
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i7.4662

attacks and the ability to persuade among users of social networking sites, where the correlation coefficient was (0.418).

The impact of awareness of social engineering attacks on the persuasion ability of social media users.

Table (1) Regression analysis to show the effect of awareness of social engineering attacks on the ability to persuade among users of social networking sites

Model		Non-standard transactions		Beta	"t"	Sig	**Correlation coefficient** (R)	**Explained contrast** ^{2}R
		Regression coefficient	Standard error					
	(Constant)	2.256	.117		19.292	.000	.418	.175
	Social engineering scale	.335	.036	.418	9.364	.000		
P value = 87.688 function at sig 0(.000)								

Dependent variable: the ability to persuade

Table (1) A significant effect (α≤0.05) exists between awareness of social engineering attacks and persuasion ability among study participants, as shown by the correlation coefficient (R) (418) and the coefficient of determination (R2), which explains 17.5% of the variance in the study.

Table (2) Differences in the ability of persuasion among users of social networking sites according to the variables of age, place of residence, economic level, educational level.

Categories	**mean**	Number	**Standard deviation**
Age			
18-20	3.38	165	.352
20-24	3.36	151	.404
Social engineering scale	3.25	99	.332
total	3.34	415	.370
Education level			
Secondary	3.32	100	.342
University	3.34	309	.379
Postgraduate	3.53	6	.329
total	3.34	415	.370
Place of residence			
North Riyadh	3.31	186	.365
Central Riyadh	3.37	126	.405
South Riyadh	3.35	88	.336
Village	3.38	15	.322
total	3.34	415	.370
Economic situation			
Less than five thousand	3.38	178	.388

Journal of Ecohumanism
2024
Volume: 3, No: 7, pp. 2580 – 2592
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i7.4662

Five to seven thousand	3.28	74	.362
More than seven thousand	3.32	163	.349
total	3.34	415	.370

It is noted from Table (2) that there are apparent differences between the arithmetic averages of the estimates of the members of the study sample about the ability to persuade, according to the variables of the study, and to determine the statistical significance of these apparent differences, the analysis of multiple quadruple variance was applied, and this is shown in Table (3)

Table (3) Multiple quadruple variance analysis to identify the differences in the ability of persuasion among users of social networking sites according to the variables of age, place of residence, economic level, educational level.

Variable	Sum of squares	Degrees of freedom	Average squares	P	sig
Age	1.247	2	.623	4.652	.010
Educational level	.602	2	.301	2.246	.107
Place of residence	.298	3	.099	.740	.529
Economic status	.500	2	.250	1.866	.156
Error	54.273	405	.134		
Total	4685.172	415			
Average Total	56.711	414			

Table (3) shows that there are no differences in the ability to persuade users of social networking sites according to variables, place of residence, economic level, educational level, and table (4) shows that there are differences according to the age variable, and to find out the significance of the differences, dimensional comparisons were made using Shafih, as follows:

Table (4) Indication of differences according to age variable by conducting dimensional comparisons using Shafih

(I) Age	(J) Age	The difference between the two averages	sig
18-20	20-24	.02	.885
	24 and up	.12(*)	.028
20-24	18-20	-.02	.885
	24 and up	.10	.089
24 and up	18-20	-.12(*)	.028
	20-24	-.10	.089

Table (4) shows the dimensional comparisons that there are differences between the category of 18-20 and the category of 24 and above and in favor of the category of 18-20 on the ability to convince totally.

Journal of Ecohumanism
2024
Volume: 3, No: 7, pp. 2580 – 2592
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i7.4662

Table (5) Differences in the level of awareness of social engineering attacks among social media users according to variables of age, place of residence, economic level, educational level

Categories	mean	N	Standard deviation
Age			
18-20	3.23	165	.479
20-24	3.23	151	.524
24 and up	3.25	99	.311
	3.23	415	.462
Education level			
Secondary	3.18	100	.399
University	3.24	309	.483
Postgraduate	3.44	6	.146
Total	3.23	415	.462
Place of residence			
North Riyadh	3.23	186	.547
Central Riyadh	3.26	126	.380
South Riyadh	3.20	88	.399
Village	3.19	15	.249
Total	3.23	415	.462
Economic situation			
Less than five thousand	3.28	178	.414
Five to seven thousand	3.18	74	.548
More than seven thousand	3.21	163	.468
Total	3.23	415	.462

It is noted from Table (5) that there are apparent differences between the arithmetic averages of the estimates of the study sample members on awareness of human engineering attacks, according to the variables of the study, and to determine the statistical significance of these apparent differences, the analysis of multiple quadruple variance was applied, and Table (6) shows that.

Table (6) Multiple quadruple variance analysis to identify differences in the level of awareness of social engineering attacks among social media users according to the variables of age, place of residence, economic level, educational level

Variable	Sum of squares	Degrees of freedom	Average squares	P	sig
Age	.081	2	.041	.190	.827
Educational level	.509	2	.254	1.188	.306
Place of residence	.202	3	.067	.314	.815
Economic status	.913	2	.456	2.131	.120
Error	86.741	405	.214		
Total	4426.607	415			

Journal of Ecohumanism
2024
Volume: 3, No: 7, pp. 2580 – 2592
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i7.4662

Average Total	88.372	414			

Table 6 shows that there are no differences in awareness of human engineering attacks according to variables, age, place of residence, economic level, and educational level.

Discussion

The study found that social networking site users' awareness of engineering attacks and persuasion ability were average, meaning they know about psychological attacks like controlling information or hacking numbers through deception, but they don't need extreme protection. Thus, they recognize threats but not for the reason that stops them from acting on them, as medium ability Give people the tools to benefit from or influence others on social media. This may hinder their ability to raise awareness or protect advanced victims. Several investigations and theoretical frameworks support this fact(Abdulla et al., 2023; Akyeşilmen & Alhosban, 2024; Albladi & Weir, 2018; Aldawood et al., 2020; Algarni, 2019; Alseadoon, 2023; Alsulami *et al.*, 2021). The study found a statistically significant positive relationship (A = 0.05) between study members' estimates of social engineering awareness and social networking users' ability to persuade, with a correlation coefficient of 0.418. Since people who care about social issues are more credible, they can influence others' perspectives. And they have Eagerness and passion for social goals urge others to interact. Socially aware persons have a greater understanding of social issues, allowing them to make stronger arguments and persuade others, as shown by Social awareness encourages people to improve their communication and expression, which increases their influence(Alsulami et al., 2021; Alzahrani, 2020; Banire et al., 2021; Bond et al., 2010; Busch et al., 2013; Chetioui et al., 2022; Cialdini, 2006; Golbeck et al., 2011; Granger, 2001; GuAdAGnO, 2013).

The study found a significant effect ($\alpha \leq 0.05$) of awareness of social engineering attacks on persuasion among study participants. This is due to improved critical thinking skills, as awareness of social engineering attacks helps individuals identify deceptive practices. This enhanced awareness stimulates critical thinking, helping people analyses information and evaluate messages. Thus, knowing these dangers helps people develop stronger arguments and counterarguments, improving their persuasiveness, and understanding social engineering strategies boosts confidence in their communication skills.

They can communicate more effectively and aggressively with this trust, enhancing their influence, Knowing social engineering strategies helps people grasp their audience's worries and weaknesses. This insight helps them personalize their communications to specific problems or misconceptions, boosting their chances of persuasion. Effective persuasion requires personal communication with the audience (Bada & Nurse, 2020; Banire et al., 2021; Bond et al., 2010; Busch et al., 2013; Chetioui et al., 2022; Cialdini, 2006; Golbeck et al., 2011; Granger, 2001; GuAdAGnO, 2013).

Social networking users may convince equally, according to for variables, put Housing, income, education, according to the researcher, social media platforms offer more uniform information availability across populations. Users can find identical material and resources regardless of geography, income, or degree. Due to the ubiquitous availability of information, consumers may be exposed to comparable persuasive strategies and arguments, reducing the impact of these variables on persuasive abilities. Social media behaviors may be governed more by online communication dynamics than by individual attributes like education or income. (Chen et al., 2021; Cialdini, 2001; Nimon-Peters, 2022; Seethaler & Rose, 2006)،.

Study reveals age-related disparities in persuasive power, with 18-20 group outperforming 24+ category. There are various reasons: Technological efficiency, trend adaptation, emotional intelligence, empathy, and emotion understanding younger generations may be more sensitive to others' sentiments and opinions, allowing them to personalise their powerful messages and establish understanding. Successful persuasion requires emotional intelligence to create audience trust and understanding., whereas cultural and social influences Influence by peers: Younger people may be more susceptible to persuasive messages and trends due to peer and societal influence, Self-discovery and identity formation may make people more open to new ideas and opinions(Krombholz et al., 2015; Matz et al., 2017; Naz et al., 2024; Nimon-Peters, 2022;

Journal of Ecohumanism
2024
Volume: 3, No: 7, pp. 2580 – 2592
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i7.4662

Orgill et al., 2004; Postnikoff & Goldberg, 2018; Salahdine & Kaabouch, 2019; Schumacher & Frühjahrsfachgespräch, 2011; Seethaler & Rose, 2006)

Lack of awareness of human engineering attacks by variables, age is a place. Social engineering affects housing, economics, and education. May boost media coverage and social media success. People of different games and social levels can be given educational information among themselves, leading to a level of awareness. The results may indicate their social or economic diversity, as it can participate in the common life bond at the consciousness level, as the engineer touches in addition to individuals. Therefore, they may share intellectual property rights on this relationship or how to recognize and handle this characteristic (Schumacher & Frühjahrsfachgespräch, 2011; Siddiqi et al., 2022; van der Kleij et al., 2023; Vishwanath, 2015; Vishwanath et al., 2018; Vrhovec, 2021)

Recommendation

1. Increase social media awareness efforts to educate young users about social engineering assaults and devise measures to protect their accounts from hackers.
2. Develop training and educational programs to improve persuasion abilities for social media users across all age groups, ensuring increased efficacy in persuading the target audience.
3. Work with educational institutions to incorporate social engineering knowledge into curricula, promote protective strategies, and include interactive activities for different age groups.

Conflict of interest

The author declare that the research was conducted without any commercial or financial relationships that could be understood as potential conflicts of interest.

References

Abdulla, R. M., Faraj, H. A., Abdullah, C. O., Amin, A. H., & Rashid, T. A. (2023). Analysis of social engineering awareness among students and lecturers. IEEE Access.

Akyeşilmen, N., & Alhosban, A. (2024). Non-Technical Cyber-Attacks and International Cybersecurity: The Case of Social Engineering. Gaziantep University Journal of Social Sciences, 23(1), 342-360.

Albladi, S. M., & Weir, G. R. (2018). User characteristics that influence judgment of social engineering attacks in social networks. Human-centric Computing and Information Sciences, 8, 1-24.

Aldawood, H., Alashoor, T., & Skinner, G. (2020). Does awareness of social engineering make employees more secure? International Journal of Computer Applications, 177(38), 45-49.

Algarni, A. (2019). What message characteristics make social engineering successful on Facebook: The role of central route, peripheral route, and perceived risk. Information, 10(6), 211.

Alseadoon, I. M. (2023). THE POWER OF INTENTION IN DETECTING SOCIAL ENGINEERING ATTACKS. International Journal on Information Technologies & Security, 15(3).

Alsulami, M. H., Alharbi, F. D., Almutairi, H. M., Almutairi, B. S., Alotaibi, M. M., Alanzi, M. E., Alotaibi, K. G., & Alharthi, S. S. (2021). Measuring awareness of social engineering in the educational sector in the kingdom of Saudi Arabia. Information, 12(5), 208.

Alzahrani, A. (2020). Coronavirus social engineering attacks: Issues and recommendations. International Journal of Advanced Computer Science and Applications, 11(5).

Bada, M., & Nurse, J. R. (2020). The social and psychological impact of cyberattacks. In Emerging cyber threats and cognitive vulnerabilities (pp. 73-92). Elsevier.

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

Bond, C., Ferraro, C., Luxton, S., & Sands, S. (2010). Social media advertising: An investigation of consumer perceptions, attitudes, and preferences for engagement. Proceedings of the Australian and New Zealand Marketing Academy (ANZMAC) Conference,

Busch, M., Schrammel, J., & Tscheligi, M. (2013). Personalized persuasive technology–development and validation of scales for measuring persuadability. International conference on persuasive technology,

Chen, S., Xiao, L., & Mao, J. (2021). Persuasion strategies of misinformation-containing posts in the social media. Information Processing & Management, 58(5), 102665.

Chetioui, K., Bah, B., Alami, A. O., & Bahnasse, A. (2022). Overview of social engineering attacks on social networks. Procedia Computer Science, 198, 656-661.

Cialdini, R. (2001). Principles of persuasion. Arizona State University, eBrand Media Publication.

Journal of Ecohumanism
2024
Volume: 3, No: 7, pp. 2580 – 2592
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i7.4662

Cialdini, R. (2006). The Psychology of Persuasion Revised Edition. In: Harper Business.
Golbeck, J., Robles, C., & Turner, K. (2011). Predicting personality with social media. In CHI'11 extended abstracts on human factors in computing systems (pp. 253-262).
Granger, S. (2001). Social engineering fundamentals, part I: hacker tactics. Security Focus, December, 18.
GuAdAGnO, R. E. (2013). Social influence online: The six principles in action. Casing persuasive communication, 319-344.
Hasan, M., Prajapati, N., & Vohara, S. (2010). Case study on social engineering techniques for persuasion. arXiv preprint arXiv:1006.3848.
Heartfield, R., & Loukas, G. (2015). A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. ACM Computing Surveys (CSUR), 48(3), 1-39.
Ivaturi, K., & Janczewski, L. (2011). A taxonomy for social engineering attacks.
Karakasiliotis, A., Furnell, S. M., & Papadaki, M. (2006). Assessing end-user awareness of social engineering and phishing.
Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and applications, 22, 113-122.
Matz, S. C., Kosinski, M., Nave, G., & Stillwell, D. J. (2017). Psychological targeting as an effective approach to digital mass persuasion. Proceedings of the national academy of sciences, 114(48), 12714-12719.
Naz, A., Sarwar, M., Kaleem, M., Mushtaq, M. A., & Rashid, S. (2024). A comprehensive survey on social engineering-based attacks on social networks.
Nimon-Peters, A. (2022). Working With Influence: Nine principles of persuasion to accelerate your career. Bloomsbury Publishing.
Orgill, G. L., Romney, G. W., Bailey, M. G., & Orgill, P. M. (2004). The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. Proceedings of the 5th conference on Information technology education,
Postnikoff, B., & Goldberg, I. (2018). Robot social engineering: Attacking human factors with non-human actors. Companion of the 2018 ACM/IEEE international conference on human-robot interaction,
Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. Future internet, 11(4), 89.
Schumacher, S., & Frühjahrsfachgespräch, G. (2011). Die psychologischen Grundlagen des Social Engineerings. Chaos, 2011, 08-11.
Seethaler, R., & Rose, G. (2006). Using the six principles of persuasion to promote travel behaviour change: Findings of a TravelSmart pilot test. Road & Transport Research: A Journal of Australian and New Zealand Research and Practice, 15(2), 94-106.
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.
Smith, A., Papadaki, M., & Furnell, S. M. (2013). Improving awareness of social engineering attacks. Information Assurance and Security Education and Training: 8th IFIP WG 11.8 World Conference on Information Security Education, WISE 8, Auckland, New Zealand, July 8-10, 2013, Proceedings, WISE 7, Lucerne Switzerland, June 9-10, 2011, and WISE 6, Bento Gonçalves, RS, Brazil, July 27-31, 2009, Revised Selected Papers 8,
Twitchell, D. P. (2006). Social engineering in information assurance curricula. Proceedings of the 3rd annual conference on Information security curriculum development,
van der Kleij, R., van 't Hoff—De Goede, S., van de Weijer, S., & Leukfeldt, R. (2023). Social engineering and the disclosure of personal identifiable information: Examining the relationship and moderating factors using a population-based survey experiment. Journal of Criminology, 56(2-3), 278-293.
Vishwanath, A. (2015). Habitual Facebook use and its impact on getting deceived on social media. Journal of Computer-Mediated Communication, 20(1), 83-98.
Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, cognition, and automaticity model of phishing susceptibility. Communication research, 45(8), 1146-1166.
Vrhovec, S. (2021). Survey about social engineering and the Varni na internetu awareness campaign, 2020. arXiv preprint arXiv:2109.00837.
Wang, Z., Sun, L., & Zhu, H. (2020). Defining social engineering in cybersecurity. IEEE Access, 8, 85094-85115.