



Fecha de presentación: 08/08/2026

Fecha de aceptación: 10/09/2026

Fecha de publicación: 01/10/2026

Lizzy Ofusori

E-mail: lizzyofusori@yahoo.co.uk

Orcid: <https://orcid.org/0000-0002-6036-619X>

Prabhakar Rontalal Subramaniam

E-mail: prabhakarr@ukzn.ac.za

Orcid: <https://orcid.org/0000-0003-2719-3503>

University of KwaZulu-Natal (UKZN). South Africa

Cita sugerida (APA, séptima edición)

Ofusori, L., & Rontalal-Subramaniam, P. (2026). Probing into the efforts in establishing trust over relationship commitment: the case of pretexting a social engineering attack. *Revista Sociedad & Tecnología*, 9(4), 525-545. DOI: <https://doi.org/10.51247/8wys1v42>

==== o ====

Analysis of trust-building efforts in relationships: the pretext attack

ABSTRACT

Social engineering represents one of the main threats to information security, exploiting psychological and behavioral factors to gain access to confidential data. Among its forms, the pretext attack stands out for its deliberate construction of credible scenarios designed to build trust and persuade victims to reveal sensitive information. The objective of this study was to analyze the influence of trust-building efforts through pretext and their relationship to the vulnerability of Information Systems and Technology students at the University of KwaZulu-Natal (UKZN) to this type of attack. The research adopted a quantitative approach, with a non-experimental, explanatory design, using a survey to collect data from Information Systems and Technology students. The data obtained were analyzed using statistical procedures to evaluate the relationship between communication quality, persuasive efforts, trust, relational commitment, and susceptibility to pretext attacks. The results showed that communication quality did not have a statistically significant influence on participants' trust. In contrast, persuasive efforts significantly increased trust, strengthening commitment in relationships and increasing vulnerability to social engineering attacks based on pretexts. It is concluded that persuasive mechanisms are a determining factor in the effectiveness of pretexts, highlighting the need to strengthen security awareness training and develop skills to identify social manipulation strategies.

Keywords: Pretext, social engineering, trust, attack cycle

==== o ====

Análisis de los esfuerzos por generar confianza en las relaciones: El caso del pretexto, un ataque de ingeniería social.

RESUMEN

La ingeniería social representa una de las principales amenazas para la seguridad de la información, al explotar factores psicológicos y conductuales para obtener acceso a datos confidenciales. Entre sus modalidades, el ataque de pretexto destaca por la construcción deliberada de escenarios creíbles que buscan generar confianza y persuadir a las víctimas para revelar información sensible. El objetivo de este estudio fue analizar la influencia de los esfuerzos por generar confianza mediante el pretexto y su relación con la vulnerabilidad de

los estudiantes de Sistemas y Tecnologías de la Información de la Universidad de KwaZulu-Natal (UKZN) frente a este tipo de ataques. La investigación adoptó un enfoque cuantitativo, con un diseño no experimental y de alcance explicativo, utilizando la técnica de encuesta para la recolección de datos entre estudiantes de Sistemas de Información y Tecnología. Los datos obtenidos fueron analizados mediante procedimientos estadísticos para evaluar la relación entre la calidad de la comunicación, los esfuerzos de persuasión, la confianza, el compromiso relacional y la susceptibilidad al ataque de pretexto. Los resultados evidenciaron que la calidad de la comunicación no ejerció una influencia estadísticamente significativa sobre la confianza de los participantes. En contraste, los esfuerzos de persuasión incrementaron significativamente la confianza, fortaleciendo el compromiso en las relaciones y aumentando la vulnerabilidad frente a los ataques de ingeniería social basados en pretextos. Se concluye que los mecanismos de persuasión constituyen un factor determinante en la efectividad del pretexto, lo que resalta la necesidad de fortalecer la formación en concienciación sobre seguridad y el desarrollo de competencias para identificar estrategias de manipulación social.

Palabras clave: Pretexto, ingeniería social, confianza, ciclo de ataque

==== o =====

Análise dos esforços de construção de confiança nas relações: o ataque de pretexto

RESUMO

A engenharia social representa uma das principais ameaças à segurança da informação, explorando fatores psicológicos e comportamentais para obter acesso a dados confidenciais. De entre as suas formas, o ataque de pretexto destaca-se pela construção deliberada de cenários credíveis, concebidos para gerar confiança e persuadir as vítimas a revelar informação sensível. O objetivo deste estudo foi analisar a influência dos esforços de construção de confiança através de pretextos e a sua relação com a vulnerabilidade dos estudantes de Sistemas de Informação e Tecnologia da Universidade de KwaZulu-Natal (UKZN) a este tipo de ataques. A investigação adotou uma abordagem quantitativa, com um desenho não experimental e explicativo, utilizando um questionário para recolher dados de estudantes de Sistemas de Informação e Tecnologia. Os dados obtidos foram analisados através de procedimentos estatísticos para avaliar a relação entre a qualidade da comunicação, os esforços persuasivos, a confiança, o compromisso relacional e a suscetibilidade a ataques de pretexto. Os resultados mostraram que a qualidade da comunicação não teve influência estatisticamente significativa na confiança dos participantes. Em contrapartida, os esforços persuasivos aumentaram significativamente a confiança, fortalecendo o compromisso nas relações e aumentando a vulnerabilidade a ataques de engenharia social baseados em pretextos. Conclui-se que os mecanismos persuasivos são um factor determinante na eficácia dos pretextos, realçando a necessidade de reforçar a formação em segurança e desenvolver competências para identificar estratégias de manipulação social.

Palavras-chave: Pretexto, engenharia social, confiança, ciclo de ataque

==== o =====

INTRODUCTION

Social engineering can be regarded as an umbrella term for computer exploitations that employ various techniques to manipulate a user. In the context of information security, social engineering can be defined as employing variety of strategies to obtain information by exploiting human vulnerability with the intention to bypass security systems (Aiden et al., 2025). According to Albladi and Weir (2018) pretexting is one of the most common form of remote social engineering attacks. Pretexting attack occurs when a hacker creates a false sense of trust between themselves and the end user by impersonating a co-worker or a figure of authority well known to an end user in order to gain access to login information. An example

of this type of scam is an email to an employee from what appears to be the head of IT support or a chat message from an investigator who claims to be performing a corporate audit. Pretexting is highly effective as it reduces human defenses to phishing by creating the expectation that something is legitimate and safe to interact with. However, while there have been several studies conducted to measure awareness of social engineering among students in tertiary institutions, there have been very few studies conducted to analyze the influence of this pretexting as a social engineering attack and its vulnerability among students in tertiary institutions, particularly in South African tertiary institutions (Chandarman & Van Niekerk, 2017).

Research rationale

With the exponential rise of technology and the Internet, students are considered one of the computer-users that is most prone to pretexting attacks. This is because, most students often carelessly surf the internet with their computer systems and spend copious amounts of time using technology (Roy, 2025). According to Perrin and Duggan (2015), approximately 85% of students across the world uses the Internet on a regular basis. The persistent psychological need to remain connected via an increasing variety of electronic devices further exposes the students to online risks (Sharma et al., 2026). Hence, it is very easy for social engineers to take advantage of inexperienced students by deceiving them into divulging confidential information or entice them to complete actions that have been compromised in a real-world setting. It should be noted that in South Africa, University of KwaZulu-Natal (UKZN) is one of the tertiary institutions that have been experiencing pretexting attacks (Adu et al., 2019). The Information & Communication Services (ICS) department in UKZN have recorded several impersonation and spoofing emails targeted to both students and staff members (Information & Communication Services, 2019). In some instances, the ICS personnel have sent warning messages to students email regarding the incoming threats (Adu et al., 2019). According to Information and Communication Services (2019) several awareness programs via webinars and on UKZN website have been organized by the ICS personnel but unfortunately, this has not completely eradicated the issue of pretexting attacks. Hence, it is essential to investigate the influence of pretexting a social engineering attack among UKZN IS&T students which this study sought to do. Thus, this study aims to answer this research question:

How do communication quality and persuasion efforts establish trust among victims?

To address the problem in focus, the hypothesis of the study is given as follows:

H₁: Communication quality and persuasion efforts has a positive influence on student's trust contributing towards students' vulnerability to pretexting as a social engineering attack.

H₀: Communication quality and persuasion efforts has a negative influence on student's trust contributing towards students' vulnerability to pretexting as a social engineering attack.

LITERATURE REVIEW

Social engineering.

There has been a massive increase in the studies related to social engineering (Albladi & Weir, 2018). This increase is due to increasing number of social engineering attacks as well as people's inability to identify the attack. In today's technologically connected society, social engineering is a threat to the security of all networks regardless of the robustness of the intrusion detection systems, cryptography methods, anti-virus software systems and firewalls (Walker, 2016). According to Broadhurst et al. (2018) humans are the weakest link in any information security systems because humans are more likely to trust other humans compared to computers or technologies. Through human interaction, an individual psychology can be maliciously exploited to divulge confidential information (Walker, 2016). Sharma et al. (2026) describes 'Social engineer' as a person that uses techniques of manipulation and

persuasion to cause individuals to divulge confidential information or complete actions that may not ultimately be in their best interest. It is important to note that one of the significant security incidents of social engineering is pretexting attack. "Social engineers" are now utilizing pretexting attacks to elicit sensitive information, and the success of this pretexting attack is determined by the response from the unsuspecting victims. Hence, this study aims to explore the influence of pretexting as a social engineering attack and its vulnerability among IS&T students at the University of KwaZulu-Natal (UKZN).

Pretexting Attack Cycle

There are nine distinct phases of pretexting attacks cycle which are: research & planning, building trust, establishing contact, engaging in conversation, extracting information, exploiting information, maintaining deception and covering tracks. Figure 1 is a representation of the attack cycle that shows the four phases.

Research and planning: Attackers conduct extensive research on their target individuals or organizations. They gather as much information as possible from various sources, such as social media, public records, or online databases, to learn about their targets' personal or professional lives (Mouton et al., 2014).

Building trust: Attackers create a believable pretext or fictional scenario to gain the trust of their targets (Mitnick & Simon, 2003). They may impersonate someone familiar, such as a colleague, customer, or authority figure, to establish credibility and lower the target's guard (Mouton et al., 2014).

Establishing contact: Attackers initiate contact with their targets through various channels, such as phone calls, emails, or in-person interactions (Butavicius et al., 2016). They carefully craft their communication to align with the pretext and gain the target's cooperation (Alseadoon, 2014).

Engaging in conversation: Attackers engage their targets in conversation to build rapport and establish a connection (Zulkurnain et al., 2015). They use social engineering techniques to manipulate emotions, exploit vulnerabilities, or extract desired information from the target (Walker, 2016).

Extracting information: Attackers gradually elicit the target's sensitive information by asking seemingly login credentials, personal details, financial information, or access to systems or resources (Walker, 2016). During this stage, the attacker typically requests certain information from the victims, stating that it is needed to confirm the victim's identity (pretexting). The attacker does this by fabricating a story that will exploit the potential victim (Zulkurnain et al., 2015).

Exploiting information: Once the attackers obtain the desired information, they leverage it to achieve their objectives. This may involve unauthorized access to systems, identity theft, financial fraud, or other malicious activities that exploit the obtained data (Alabdan, 2020).

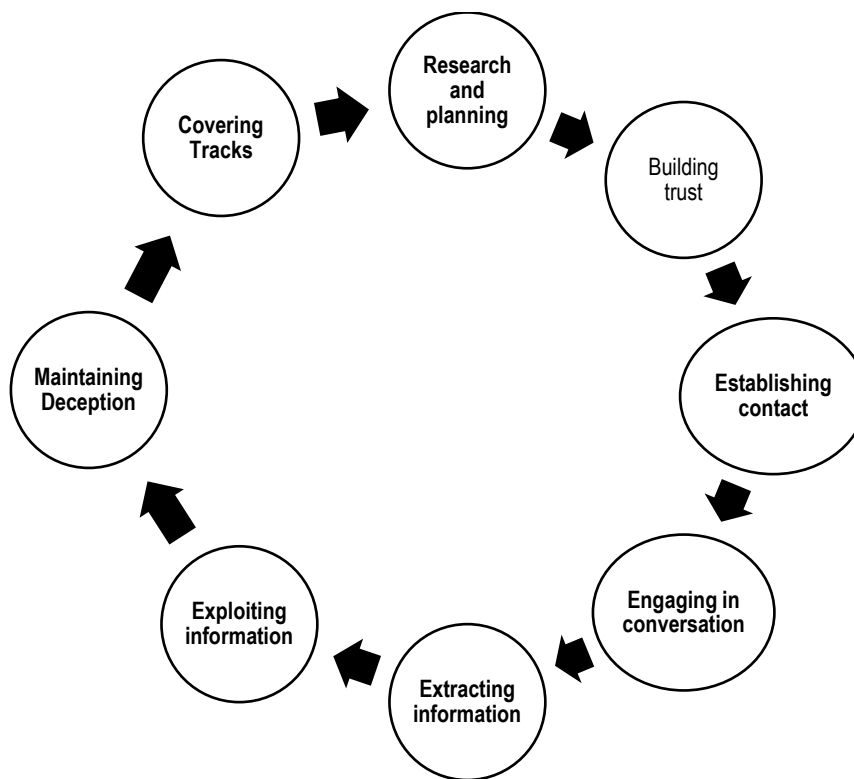
Maintaining Deception: To prolong the success of the attack, attackers ensure they maintain the deception (Alabdan, 2020). They may continue to engage in ongoing communication, monitor the target's behaviour, and adapt their pretext if necessary to avoid raising suspicion (Alseadoon, 2014).

Covering Tracks: After achieving their goals, attackers attempt to cover their tracks to evade detection. They may erase evidence of their communication, obfuscate their identity, or take steps to prevent their activities from being traced back to them (Mitnick & Simon, 2003).

Understanding the pretexting attack cycle can help individuals and organizations recognize and respond to such attacks. It is crucial to maintain a healthy skepticism, verify requests for sensitive information, and establish clear protocols for information sharing to mitigate the risk of falling victim to pretexting attacks.

Figure 1

Pretexting attack cycle (Author's own)



Related techniques used to influence

In social engineering attack, a range of techniques is used to influence people to respond, such as scarcity, sense of urgency and reciprocity (Sharma et al., 2026).

The principle of scarcity can be defined on “the idea that people will alter their behaviour when pursuing a scarce resource” (Stergiou, 2013, p. 4). This implies that when scarcity is perceived, demand automatically increase. According to Tian et al. (2018), when the availability of a product is limited in terms of quantities, it becomes far more desirable than when it is available in abundant quantities.

The principle of “sense of urgency” has to do with social engineers instilling fear in their victim so they could rush to action and overlook the potential red flags that they might be dealing with someone who is not legitimate (Lord, 2020, p. 1). Social engineers often send emails or text messages aimed at creating a sense of urgency, fear or curiosity in victims, leading the victim to promptly reveal sensitive information, open a malicious file, or click a malicious link (Alseadoon, 2014; Lord, 2020).

Reciprocity can be defined as the act of repaying someone that does something nice for you (Walker, 2016). It is a social norm where someone feel obligated to return the favour done to him/her to the person that did the favour (Stergiou, 2013). An attacker may try to do something for the victim before requesting for a favour in return (Tian et al., 2018).

Research model

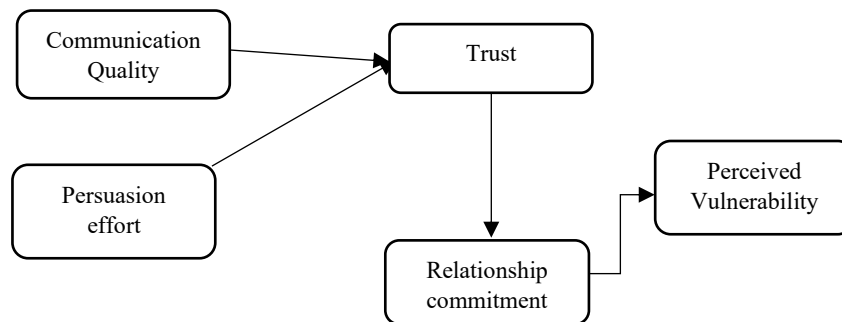
There are several theories and models in information systems that have been developed to understand the important factors associated with the influence of social engineering attacks and its vulnerability. These theories include Interpersonal deception theory (IDT), Equity

theory, Social Exchange Theory (SET) and Commitment-Trust Theory. According to Hargie (2016), IDT mostly uses facial signals or face to face communication in explaining processes and outcome of deception. Whereas equity theory simply focuses on issues of inequity and how people respond to and manage those situations in which they feel their costs are greater than the rewards (Adams & Freedman, 1976). On the other hand, Social Exchange Theory is a paradigm of tenets and assumptions that often involves social exchanges where people are motivated to attain some valued reward for which they must forfeit something of value (cost) (Redmond, 2015). Similarly, Commitment-Trust Theory focus on how strong the relationship between customer and a buyer are maintained opportunistically (Morgan & Hunt, 1994).

This study adopts SET in investigating communication quality, persuasive efforts and trust because it captures the cognitive behaviour of the sender as it relates to social engineering attack. In addition, the study adopts Commitment-Trust Theory to investigate relationship commitment as it relates to expectations and relationship satisfaction from the receiver side. The illustration is given in Figure 2.

Figure 2

Conceptual model (Author's own)



Source: Own elaboration

The relationship between communication quality and trust is rather a fundamental human psychological process whose effects frequently appear in inter-organizational B2B relationships (Ball et al., 2004; Jeong & Oh, 2017). In the same vein, social engineers also introduce a positive relationship of communication quality in order to establish trust. Bhattacharjee and Sanford (2006) affirm that an individual is most likely to trust an email/messages when the content is error free and professional, thus making the individual vulnerable to attack. Other factors that contribute to communication quality include source credibility, argument quality and authority. It should be noted that social engineers introduce a positive communication quality to establish trust with the targeted students. According to Alseadoon (2014) the way we communicate with others is a primary way we build trust. In the same vein, social engineers also introduce a positive connection among communication quality to establish trust.

The success of persuasion effort depends on the impact of a message on evoking thoughts that are compelling to the user (Cropanzano et al., 2017). A social engineer seizes every opportunity to persuade and to positively influence the development of trust in order to achieve their selfish goals. Although this may damage the partner's long-term commitment to the relationship when the partner discovers he/she is being exploited (Jeong & Oh, 2017). In the same vein, social engineers also introduce a positive relationship of persuasion effort in order to establish students' trust.

Trust is defined as “the belief in an exchange partner’s reliability and integrity in fulfilling relational obligations and it reflects the degree to which dyadic partners perceive each other as credible and benevolent” (Jeong & Oh, 2017). Establishing trust can take different forms such as perceived reputation, website trustworthiness and structural assurance (Walker, 2016). Hence, in the context of this study, as trust relationship strengthens, it also tends to affect the students’ response towards relationship commitments.

Relationship commitment is the key factor in building and maintaining good relationships (Huo et al., 2015). As a result, customers tended to view potential risk options as prudent because of the perception that their partners would not act opportunistically (Morgan & Hunt, 1994). A committed relationship is based upon commitment to one another involving trust, openness, honesty or some other behaviour (Abdullah & Musa, 2014). Hence, in the context of this study, as relationship commitment strengthens, it also tends to make the students’ vulnerable to pretexting as a social engineering attack.

Perceived vulnerability is the individual's judgment regarding the likelihood that the threat would occur (Benavides-Astudillo et al., 2021). According to Hameed and Arachchilage (2019), it is an assessment to measure the scale of a threat's exposure done by an individual. Hence, in the context of this study, perceived vulnerability represents a negative consequence resulting from relationship commitment.

Research methodology and data analysis

This study follows an empirical approach with the aid of collecting data from a reasonably large sample and uses statistical analysis to offer a complete investigation on how communication quality and persuasion efforts influence student’s trust contributing towards relationship commitment leading to students’ vulnerability to pretexting. The study adopts a survey research strategy because they are mostly used in social science to collect quantitative data (Bryman & Bell, 2011). The quantitative approach was found to be most effective in gathering data from the students. It is very flexible and is often utilized to collect different types of information ranging from small to large populations (Bryman & Bell, 2011).

The estimated population in IS&T qualification is a total of 90 for the three different levels. Using the information gained in the university Moodle platform, the first year consisted of 45 students, the second year had 25 students and third-year had 20 students as at the first quarter of 2021 in UKZN, Durban. This study used a stratified random sampling technique in determining the sample size for each stratum. Based on the first rule of thumb for selecting an appropriate sample size proposed by Krejcie and Morgan (1970) as cited by Daniel and Cross (2018), the researcher used the following parameters of 95% confidence level, sample proportion of 0.5, margin error of 0.05 to calculate the sample size for each stratum. Hence, first year sample size for a population size of 45 is 40. The second-year sample size for a population of 25 is 24 while the third-year sample size for a population of 20 is 17. Thus, the total sample size for this study is 81. This decision was supported by the Table of minimum sample sizes for different population sizes at a 95 per cent confidence level. The study is guided by the ethical clearance provided by UKZN. All the information provided by the participants was treated as confidential and was not divulged to any third party

Data collection techniques

In this study, a quantitative approach using a questionnaire was adopted for collecting data. The questionnaire was designed using google form to collect quantitative data. When the sample size was reached, the google form was closed. Google form was used because this research was done during the COVID-19 period that requires everyone to comply with the COVID-19 regulations. Also, the outcome of the study was analysed with a statistical analysis SPSS tool that examines the relationship of variables that are considered in this research work

The questionnaire was made up of six sections (Sections A, B, C, D, E and F). Sections A examines the demographic of the students. Sections B, C, D and E investigates students’

perceptions on pretexting attack and also examines factors contributing to perceived vulnerability. While Section F measures students' vulnerability to pretexting a social engineering attack using non-parametric tests. The questionnaire items used are shown in Appendix.

In ensuring validity, questionnaires designed by the researcher was compared to other validated questionnaires using the content validity technique. Experts in the subject matter were granted access to the questionnaire and requested to give input on how well each of the questions was aligned and addresses each construct in the questions. Hence, the feedback was analyzed, and this was used to decide the effectiveness of all the question. In addition, a pilot test was carried out on the research instruments to elicit dependable responses from a selected sample. The researcher selected 8 participants for the pilot test which represented approximately 10% of the sample size. This was to check for clarity and to test whether the participants understood what was expected of them. The response obtained from the pilot test gave clarification, correction and ideas that were used to improve the questionnaires.

Likewise, the internal consistency reliability was tested using the Cronbach's alpha as a reliability indicator for this study. Table 1 shows the reliability coefficients calculated for the study. According to Tavakol and Dennick (2011), any alpha value greater than 0.7 (out of 1) is acceptable since it shows that the study variables measure what they are intended to measure. The highest reliability coefficient for this study was on communication quality, with an alpha value of 0.796 while Trust value was lowest, with an alpha of 0.717. All variables were considered to be reliable based on the coefficients calculated.

Table 1

Reliability test on variables considered in this study

Variable	Cronbach's alpha	Remarks
Communication quality	0.796	Acceptable
Persuasion effort	0.755	Acceptable
Trust	0.717	Acceptable
Relationship commitment	0.792	Acceptable

Source: Own elaboration

Data analysis and results

The sample is composed of 40% male and 60% female. Additionally, the sample was composed of various age groups; majority were between the age of 21- 22 years (38.3%), 25 years and above (25.9%), 19-20 (18.5%), 23-24 (8.6%) and 18 years were only 8.6%. Likewise, majority of students were from College of Law and Management studies (65.4%), followed by Agriculture, Engineering and Sciences (29.6%), Humanities (3.7%) and Health science (1.2%). Also, the sample was composed of the year of study; majority are 3rd year students (45%), 1st year (12%), 2nd year students (6%) and others (37%).

Similarly, students were assessed on their availability on social media; 82.7% students said they are available on social media regularly, while 17.3% said they are not. In addition, 95.1% students noted that they are aware of personal and privacy security threats on social media, while 4.9% said they are not. Also, 42% of the students affirmed that they have previously experienced security threats on social media, while 58% said they have not. Data was analysed using the Statistical Package for the Social Sciences (SPSS). First, students' perceptions on receiving social media security threats were determined and inferential analysis comprises of an independent samples t-test and non-parametric tests was used to establish the impact of persuasion and responses on pretexting attacks, based on the pre-determined factors. The students' perceptions consisted of 5 items measured on a 5-point Likert scale, ranging from 1 = strongly disagree, to 5 = strongly agree. Likewise, a non-parametric (The Man-Whitney U) test was conducted as a complement to the independent

samples t-test and sought to establish the factors influencing students' vulnerability to social engineering threats as it relates to pretexting, where data was assumed not to be normally distributed. According to MacFarland and Yates (2016) the Mann-Whitney U test is used to compare two independent samples when the outcome is not normally distributed and the samples are small.

Students' perceptions on pretexting: A social engineering attack

This section presents descriptive data on students' perceptions on pretexting, a social engineering attack. The section interrogates how two elements of trust; communication quality and persuasion efforts are likely influence how individuals build trust leading towards relationship commitment with potential sources of threats. Student perceptions were measured by ascertaining the level of agreement or disagreement of respondents on the items that were used to measure communication quality and persuasion effort.

Communication quality

The effective connection among communication quality and trust is a fundamental human psychological process whose frequent effects appear in inter-organizational B2B relationships (Ball et al., 2004; Jeong & Oh, 2017). Participants were provided with a series of scenarios measuring communication quality and asked to indicate their agreement or disagreement levels. As indicated on Table 2, scenario 1.1 suggests that a student would respond to emails if the language used appears grammatically correct, 9.9% disagreed and strongly disagreed, 65.5% agreed and strongly agreed, while 24.7% were neutral. Similarly, scenario 1.2 indicate that students would respond to emails if it has the organization's logo or trademark, 4.9% disagreed and strongly disagreed, 72.8% agreed and strongly agreed, and 22.2% were neutral. Likewise scenario 1.3 indicate that students would respond to emails with informative content, 9.8% disagreed and strongly disagreed, 64.2% agreed and strongly agreed, while 25.9% were neutral. Also, scenario 1.4 suggest that a student would respond to emails related to career development, 5% disagreed and strongly disagreed, 80.3% agreed and strongly agreed, while 14.8% were neutral. Lastly, scenario 1.5 indicate that a student would respond to emails with attachment, 14.8% disagreed and strongly disagreed, 64.2% agreed and strongly agreed, while 21.0% were neutral. Overall, 69.4% of participants agreed and strongly agreed with the suggested scenarios, 8.9% disagreed and strongly disagreed, while 21.7% were neutral. Descriptive data on communication quality suggests that on average, students are more likely to fall prey to pretexting a social engineering attack if they perceived that the email received to be related to career development. Career development was most highly rated as a convincing part of a message; while informative content and email with attachments was rated last. Supporting this findings, Mouton et al. (2016) affirm that the "pretexter" often come up with clever methods such as free workshops, seminars related to career development that requires the victim to register by providing personal information. According to Conteh (2021) the attacker creates a fabricated scenario to obtain privileged data about the victim in order to engage in identity theft or corporate espionage.

Persuasion effort

The success of persuasion effort depends on the impact of a message on evoking thoughts that are compelling to the user (Cropanzano et al., 2017). Participants were provided with a series of scenarios measuring communication quality and asked to indicate their agreement or disagreement levels. As indicated on Table 2, scenario 2.1 suggest that a student would respond to emails if the sender attaches monetary benefits, 62.9% disagreed and strongly disagreed, 14.8% agreed and strongly agreed, while 22.2% were neutral. Similarly, scenario 2.2 suggest that students would respond to emails requesting for account verification, 59.3% disagreed and strongly disagreed, 25.9% agreed and strongly agreed, and 14.8% were neutral. Likewise, scenario 2.3 indicate that students would respond to emails with advertised free antivirus, 81.5% disagreed and strongly disagreed, 8.6% agreed and strongly agreed, while 9.9% were neutral. Also, scenario 2.4 suggest that a student would respond to emails

with links for advertised products, 74.1% disagreed and strongly disagreed, 13.6% agreed and strongly agreed, while 12.3% were neutral. Lastly, scenario 2.5 indicate that a student would respond to emails from a known person, 49.4% disagreed and strongly disagreed, 24.7% agreed and strongly agreed, while 25.9% were neutral. Overall, 17.5% of participants agreed and strongly agreed with the suggested scenarios, 65.4% disagreed and strongly disagreed, while 17.0% were neutral. Descriptive data on persuasion effort suggests that on average, 17.5% of students are more likely to fall prey to pretexting if they are persuaded. Emails requesting for account verification was most highly rated; while emails with advertised free antivirus was rated last.” Corroborating this findings Mouton et al. (2016) argue that the attacker will be able to gain access to the victim’s e-mail account after a successful request for a password reset or account verification for which the victims complies.

Trust

Establishing trust can take different forms such as website trustworthiness, structural assurance, perceived reputation (Walker, 2016). Participants were provided with a series of scenarios measuring trust and asked to indicate their agreement or disagreement levels. As indicated on Table 2, scenario 3.1 suggest that students are more likely to trust the email sender if it comes from a source that looks genuine, 13.6% disagreed and strongly disagreed, 46.9% agreed and strongly agreed, while 39.5% were neutral. Similarly, scenario 3.2 suggest that students are more likely to trust the email sender if the communication is repeated periodically, 39.5% disagreed and strongly disagreed, 23.5% agreed and strongly agreed, and 37.0% were neutral. Likewise, scenario 3.3 suggest that students are more likely to trust the email sender if the identity is familiar, 9.9% disagreed and strongly disagreed, 79% agreed and strongly agreed, while 11.1% were neutral. Also, scenario 3.4 suggest that students are more likely to trust the email sender if the content of the email increases their confidence, 23.5% disagreed and strongly disagreed, 40.7% agreed and strongly agreed, while 35.8% were neutral. Lastly, scenario 3.5 indicate that students are more likely to trust the email sender if they are expecting some information, 6.1% disagreed and strongly disagreed, 82.7% agreed and strongly agreed, while 11.1% were neutral. Overall, 54.5% of participants agreed and strongly agreed with the suggested scenarios, 18.5% disagreed and strongly disagreed, while 26.9% were neutral. Descriptive data on trust suggests that on average, students are more likely to fall prey to pretexting if they trust the sender of the email. Students expecting some information was most highly rated; while repeated communication was rated last.

Relationship commitment

Relationship commitment is the key factor in building and maintaining good relationships. As a result, customers tended to view potential risk options as prudent because of the perception that their partners would not act opportunistically (Morgan & Hunt, 1994). As indicated on Table 2, scenario 4.1 suggest that a student would respond to emails if they feel obliged to execute a request, 21% disagreed and strongly disagreed, 44.5% agreed and strongly agreed, while 34.6% were neutral. Similarly, scenario 4.2 suggest that students are willing to motivate friends to respond for rewards, 53% disagreed and strongly disagreed, 19.7% agreed and strongly agreed, and 27.2% were neutral. Likewise, scenario 4.3 indicate that students are determined to motivate family to respond for recognition, 45.7% disagreed and strongly disagreed, 19.7% agreed and strongly agreed, while 34.6% were neutral. Also, scenario 4.4 suggest that students are convinced to respond to emails that looks like a legitimate sender, 25.9% disagreed and strongly disagreed, 43.2% agreed and strongly agreed, while 30.9% were neutral. Lastly, scenario 4.5 suggest that students are willing to be open-minded when communicating, 17.3% disagreed and strongly disagreed, 51.8% agreed and strongly agreed, while 30.9% were neutral. Overall, 35.7% of participants agreed and strongly agreed with the suggested scenarios, 32.4% disagreed and strongly disagreed, while 31.6% were neutral. Descriptive data on relationship commitment suggests that on average, students are more likely to fall prey to pretexting if relationship commitment is

established. Students been open-minded when communicating was most highly rated; while motivating friends and family was rated last.

Perceived vulnerability

Perceived vulnerability can be described as individual's judgment concerning the possibility of the threat happening (Garcia et al., 2018). Participants were provided with a series of scenarios measuring perceived vulnerability and asked to indicate their agreement or disagreement levels. As indicated on Table 2, scenario 5.1 suggest the susceptibility of students to hackers if they reveal personal information, 1.2% disagreed and strongly disagreed, 96.3% agreed and strongly agreed, while 2.5% were neutral. Similarly, scenario 5.2 indicate that if students motivate friends to respond for rewards they are likely to fall a prey to fraudulent act, 0.0% disagreed and strongly disagreed, 95% agreed and strongly agreed, while 4.9% were neutral. Likewise, scenario 5.3 suggest that students that if students motivate family to respond for recognition, they are likely to be vulnerable to hackers, 1.2% disagreed and strongly disagreed, 95% agreed and strongly agreed, while 3.7% were neutral. Also, scenario 5.4 indicate that students are more likely to fall a prey to fraudulent act if they respond to the sender of email without verifying the legitimacy of the sender's company, 1.2% disagreed and strongly disagreed, 95% agreed and strongly agreed, while 3.7% were neutral. Lastly, scenario 5.5 suggest that students could be vulnerable to attack when they are open-minded in communication, 1.2% disagreed and strongly disagreed, 90.1% agreed and strongly agreed, while 8.6% were neutral. Overall, 94.2% of participants agreed and strongly agreed with the suggested scenarios, 1% disagreed and strongly disagreed, while 4.7% were neutral. Descriptive data on perceived vulnerability suggests that on average, students are more aware of the possibilities of being susceptible to pretexting, a social engineering attack. Susceptibility of students to hackers if they reveal personal information is highly rated; while been open-minded in communication was rated last. It should be noted that some students chose the "neutral" option. Such students can be considered as not been aware of the risks associated with social engineering attack which can be seen as a serious threat.

Table 2

Perceptions of students on pretexting: A social engineering attack

1	I would respond to	Communication quality				
		Percentage of students				
		SD	D	N	A	SA
1.1	email/message if the language used in the email/message appears grammatically correct (i.e., error-free messages)	3.7	6.2	24.7	38.3	27.2
1.2	emails that have an organization's logo and trademarks that accompanies the email	1.2	3.7	22.2	37.0	35.8
1.3	email/message if the content of the email/message is informative	4.9	4.9	25.9	42.0	22.2
1.4	email/message if the content of the email/message is related to my career development (e.g., workshops, seminars)	2.5	2.5	14.8	45.7	34.6
1.5	email/message that comes with an attachment with the supportive information of the email	3.7	11.1	21.0	39.5	24.7
	Overall	3.2	5.7	21.7	40.5	28.9
2	I am likely to respond to	Persuasion efforts				
		Percentage of students				
		SD	D	N	A	SA

2.1	email/message if the sender attaches monetary benefits that requires me to claim within a specified time	33.3	29.6	22.2	12.3	2.5
2.2	email/message prompting me to verify my account information (e.g., username and password)	39.5	19.8	14.8	18.5	7.4
2.3	pop up messages telling me that my computer has been infected with viruses and convincing me to use the advertised antivirus for free to fix the problem	54.3	27.2	9.9	3.7	4.9
2.4	email/message prompting me to click on a link for more information on their advertised products	49.4	24.7	12.3	11.1	2.5
2.5	email/message requests from a known person outside the organization.	27.2	22.2	25.9	17.3	7.4
	Overall	40.7	24.7	17.0	12.6	4.9
	Trust					
3	I am likely to trust the email sender when	Percentage of students				
		SD	D	N	A	SA
3.1	the email/message that requires a sense of urgency if it comes from a source that looks genuine (e.g. URL with https)	3.7	9.9	39.5	37.0	9.9
3.2	the email/message if the communication is repeating periodically	9.9	29.6	37.0	17.3	6.2
3.3	the email/message if the sender's identity is familiar to me	3.7	6.2	11.1	66.7	12.3
3.4	the email/message if the content of the email/message is written in such a way that it increases my confidence of executing what is requested	3.7	19.8	35.8	35.8	4.9
3.5	the email/message from a sender if I am expecting some information (e.g. confirmation of job offer)	1.2	4.9	11.1	44.4	38.3
	Overall	4.4	14.1	26.9	40.2	14.3

Source: Own elaboration

Table 2

Perceptions of students on pretexting: A social engineering attack Contd...

4.	Relationship commitment					
	I am	Percentage of students				
		SD	D	N	A	SA
4.1	willing to respond to email/messages if I feel obliged to execute the request	6.2	14.8	34.6	34.6	9.9
4.2	willing to motivate my friends to respond for rewards	16.0	37.0	27.2	14.8	4.9
4.3	determined to motivate my family to respond for recognition	17.3	28.4	34.6	16.0	3.7
4.4	convinced to respond to email/messages that looks like a legitimate sender (e.g., standardbank.co. za, gtbank.com)	8.6	17.3	30.9	35.8	7.4
4.5	willing to be open-minded when communicating with the sender of the email/message	3.7	13.6	30.9	37.0	14.8
	Overall	10.4	22.2	31.6	27.6	8.1

5	I am aware that if I	Perceived vulnerability				
		Percentage of students				
		SD	D	N	A	SA
5.1	reveal personal information to fulfil my interest, I could be susceptible to hackers	-	1.2	2.5	33.3	63.0
5.2	motivate my friends to respond for rewards, they could fall prey to fraudulent act	-	-	4.9	37.0	58.0
5.3	motivate my family to respond for recognitions, they could be vulnerable to hackers	-	1.2	3.7	33.3	61.7
5.4	respond to emails/messages without verifying the legitimacy of the sender's company, I could fall prey to fraudulent act	-	1.2	3.7	29.6	65.4
5.5	am open-minded when communicating with the sender of the email/message I could be vulnerable to attack	-	1.2	8.6	37.0	53.1
	Overall	0	1.0	4.7	34.0	60.2

Source: Own elaboration

Descriptives

On Table 3, descriptives on communication quality show that the modal choice for students was 4, associated with the 'Agree' option. This shows that on average, the students are likely to trust emails they receive as long as they trust the quality of communication used. The means were 3.79, 4.02, 3.72, 4.07 and 3.70, associated with scenarios 1.1, 1.2, 1.3, 1.4, and 1.5 respectively. Meanwhile, the standard deviation on the first case was 1.033, 0.922 for the second case, 1.028 for the third case, 0.905 for the fourth case, and 1.078 for the fifth case. It can be seen that the greatest variability in views was on the fifth scenario (quality of supporting information/ attachment) and lowest on the fourth scenario (email content relating to career development).

Similarly, on Table 3, descriptive on persuasion efforts show that the modal choice for students was 1, associated with the 'Strongly disagree' option. This shows that on average, the students are not likely to succumb to persuasion efforts even when they trust the quality of communication used and the sender's behaviour. The means and standard deviation were used to describe the weight of each scenario and to compare students' ratings. The mean and standard deviation associated with scenario 2.1 were mean=2.21, SD=1.115. For scenario 2.2, the mean and standard deviation were mean=2.35, SD=1.362. For scenario 2.3, the mean and standard deviation were mean=1.78, SD=1.095. For scenario 2.4, the mean and standard deviation were mean=1.93, SD=1.138. Lastly, scenario 2.5, the mean and standard deviation were mean=2.56, SD=1.265. It can be seen that the greatest variability in views was on the fifth scenario (email request from a known person) and lowest on the third scenario (advertised free antivirus).

On Table 3, descriptives on trust show that the modal choice for students was 3, associated with the 'Neutral' option. This shows that on average, the students are likely or unlikely to trust the email sender regardless of the quality of communication used and the persuasion efforts from the sender. The means were 3.40, 2.80, 3.78, 3.19 and 4.14, associated with scenarios 3.1, 3.2, 3.3, 3.4, and 3.5 respectively. Meanwhile, the standard deviation on the first case was 0.931, 1.042 for the second case, 0.880 for the third case, 0.937 for the fourth case, and 0.891 for the fifth case. It can be seen that the greatest variability in views was on the fifth scenario (expecting some information) and lowest on the second scenario (communication is repeated periodically).

Likewise, on Table 3, descriptive on relationship commitment show that the modal choice for students was 4, associated with the 'Agree' option. This shows that on average, the students are likely to commit to a relationship with the sender of the emails as long as they trust the quality of communication used and the persuasion efforts. The means and standard deviation were used to describe the weight of each scenario and to compare students' ratings. The mean and standard deviation associated with scenario 4.1 were mean=3.27, SD=1.037. For scenario 4.2, the mean and standard deviation were mean=2.56, SD=1.084. For scenario 4.3, the mean and standard deviation were mean=2.60, SD=1.069. For scenario 4.4, the mean and standard deviation were mean=3.16, SD=1.078. Lastly scenario 4.5, the mean and standard deviation were mean=3.46, SD=1.025. It can be seen that the greatest variability in views was on the fifth scenario (willing to be open minded when communicating) and lowest on the second scenario (willing to motivate friends to respond for rewards).

In addition, On Table 3, on perceived vulnerability show that the modal choice for students was 5, associated with the 'Strongly Agree' option. This shows that on average, the students are likely not to be vulnerable to social engineering attack. The means were 4.58, 4.53, 4.56, 4.59 and 4.42, associated with scenarios 5.1, 5.2, 5.3, 5.4, and 5.5 respectively. Meanwhile, the standard deviation on the first case was 0.610, 0.593 for the second case, 0.632 for the third case, 0.628 for the fourth case, and 0.705 for the fifth case. It can be seen that the greatest variability in views was on the fourth scenario (verifying the legitimacy of the sender's company) and lowest on the fifth scenario (open-minded when communicating).

Table 3

Descriptive analysis on students' perceptions on pretexting: A social engineering attack

Communication quality				
	I would respond to	Mean	Mode	Standard Deviation
1.1	email/message if the language used in the email/message appears grammatically correct (i.e., error-free messages)	3.79	4	1.033
1.2	emails that have an organization's logo and trademarks that accompanies the email	4.02	4	0.922
1.3	email/message if the content of the email/message is informative	3.72	4	1.028
1.4	email/message if the content of the email/message is related to my career development (e.g., workshops, seminars)	4.07	4	0.905
1.5	email/message that comes with an attachment with the supportive information of the email	3.70	4	1.078
Persuasion efforts				
2	I am likely to respond to	Mean	Mode	Standard Deviation
2.1	email/message if the sender attaches monetary benefits that requires me to claim within a specified time	2.21	1	1.115
2.2	email/message prompting me to verify my account information (e.g., username and password)	2.35	1	1.362
2.3	pop up messages telling me that my computer has been infected with viruses and convincing me to use the advertised antivirus for free to fix the problem	1.78	1	1.095
2.4	email/message prompting me to click on a link for more information on their advertised products	1.93	1	1.138
2.5	email/message requests from a known person outside the organization.	2.56	1	1.265

Source: Own elaboration

Table 3

Descriptive analysis on students' perceptions on pretexting: A social engineering attack Contd...

Trust				
3	I am likely to trust the email sender when	Mean	Mode	Standard Deviation
3.1	the email/message that requires a sense of urgency if it comes from a source that looks genuine (e.g. URL with https)	3.40	3	0.931
3.2	the email/message if the communication is repeating periodically	2.80	3	1.042
3.3	the email/message if the sender's identity is familiar to me	3.78	4	0.880
3.4	the email/message if the content of the email/message is written in such a way that it increases my confidence of executing what is requested	3.19	3	0.937
3.5	the email/message from a sender if I am expecting some information (e.g. confirmation of job offer)	4.14	4	0.891
Relationship commitment				
4	I am	Mean	Mode	Standard Deviation
4.1	willing to respond to email/messages if I feel obliged to execute the request	3.27	3	1.037
4.2	willing to motivate my friends to respond for rewards	2.56	2	1.084
4.3	determined to motivate my family to respond for recognition	2.60	3	1.069
4.4	convinced to respond to email/messages that looks like a legitimate sender (e.g., standardbank.co. za, gtbank.com)	3.16	4	1.078
4.5	willing to be open-minded when communicating with the sender of the email/message	3.46	4	1.025
Perceived vulnerability				
5	I am most likely to	Mean	Mode	Standard Deviation
5.1	reveal personal information to fulfil my interest, I could be susceptible to hackers	4.58	5	0.610
5.2	motivate my friends to respond for rewards, they could fall prey to fraudulent act	4.53	5	0.593
5.3	motivate my family to respond for recognitions, they could be vulnerable to hackers	4.56	5	0.632
5.4	respond to emails/messages without verifying the legitimacy of the sender's company, I could fall prey to fraudulent act	4.59	5	0.628
5.5	am open-minded when communicating with the sender of the email/message I could be vulnerable to attack	4.42	5	0.705

Source: Own elaboration

Measuring vulnerability on pretexting using Independent samples t-tests

An independent samples t-test is important in exploring how the mean of communication quality and persuasion effort, and trust among other factors compares with the mean of students' perceived vulnerability. Results of the tests are shown as follows (refer Table 4)

Table 4:

Independent samples t-tests

Variable	Test value (t)	d.f.	Significance value	Decision on H_0
Communication quality	0.413	8.306	0.690	Do not reject
Persuasion effort	-2.953	8.447	0.017*	Reject
Trust	-3.167	8.857	0.012*	Reject
Relationship commitment	-2.495	11.597	0.029*	Reject

* Test results are significant at the 95% confidence level

Table 4 results on communication quality showed a test value of 0.413, 8.306 degrees of freedom and $p = 0.690$. This result does not reject the null hypothesis ($p < 0.05$), concluding that communication quality does not significantly explains students' perceived trust. Similarly, results on persuasion effort showed a test value of -2.953, 8.447 degrees of freedom and $p = 0.017$. This result rejected the null hypothesis ($p < 0.05$) at the 95% confidence level, concluding that the persuasion effort variable significantly explains students' perceived trust. In addition, results on trust showed a test value of -3.167, 8.857 degrees of freedom and $p = 0.012$. This result rejected the null hypothesis ($p < 0.05$) at the 95% confidence level, concluding that the trust variable significantly explains students' relationship commitment leading towards perceived vulnerability. Likewise, results on the association between relationship commitment and perceived vulnerability produced a test value of -2.495, 11.597 degrees of freedom, and a p value of 0.029. This result rejected the null hypothesis at the 95% confidence level, confirming that relationship commitment was significantly associated with perceived vulnerability to social engineering attacks. This shows that three factors (persuasion effort, trust and relationship commitment) were found to significantly affect students' perceived vulnerability, as per the independent samples t-test. Hence, the hypothesis H_1 is now modified to exclude communication quality as illustrated below:

H_1 : Persuasion effort has a positive influence on student's trust contributing towards relationship commitment leading to perceived vulnerability to pretexting attack.

Man-Whitney U test results

Non-parametric test (The Man-Whitney U test) was conducted as complement to the independent samples t-test and sought to establish the factors influencing students' vulnerability to pretexting, a social engineering attack, where data was assumed not to be normally distributed. The Man-Whitney U test, show, per variable, how individuals with different views on factors perceived their vulnerability to social engineering attacks (refer Table 5).

Table 5

Man-Whitney U test results

Variable	Test value (t)	Significance value	Decision on H_0
Communication quality	267.5	0.696	Do not reject
Persuasion effort	125.5	0.008**	Reject
Trust	119.5	0.006**	Reject
Relationship commitment	167.0	0.047*	Reject

* Test results are significant at the 90% confidence level

** Test results are significant at the 99% confidence level

The Man-Whitney U test (refer Table 5) results, on communication quality showed a test value of 267.5, and $p = 0.696$. This result does not reject the null hypothesis ($p < 0.05$), concluding that communication quality does not significantly explains students' perceived vulnerability. Similarly, results on persuasion effort showed a test value of 125.5, and $p = 0.008$. This result rejected the null hypothesis ($p < 0.05$) at the 99% confidence level, concluding that persuasion effort variable significantly explains students' perceived vulnerability. In addition, results on trust showed a test value of 119.5, and $p = 0.006$. This result rejected the null hypothesis ($p < 0.05$) at the 99% confidence level, concluding that the trust variable significantly explains students' perceived vulnerability. Likewise, results on relationship commitment showed a test value of 167.0, and $p = 0.047$. This result rejected the null hypothesis ($p < 0.05$) at the 90% confidence level, concluding that the relationship commitment variable significantly explains students' perceived vulnerability

DISCUSSION

The study employed an independent samples t-test to establish the impact of persuasion and responses on pretexting, a social engineering attack, based on the pre-determined variables (communication quality, persuasion effort, trust and relationship commitment). All variables rejected the null hypothesis ($p < 0.05$) at the 99% confidence level except for communication quality as shown in Table 4. This implies that persuasion effort has a positive influence on student's trust contributing towards relationship commitment leading to students' vulnerability to social engineering attacks. Corroborating this findings, Cropanzano et al. (2017) affirm that a social engineer seizes every opportunity persuade and to positively influence the development of trust in order to achieve their selfish goals. Although this may damage the partner's long-term commitment to the relationship when the partner discover he/she is being exploited (Jeong & Oh, 2017).

To complement the independent samples t-test which sought to establish the factors influencing students' vulnerability to social engineering attacks, where data was assumed not to be normally distributed, a non-parametric test (i.e., the Man-Whitney U test) was run. In the Man-Whitney U test, all variables rejected the null hypothesis except communication quality (refer section 4.1.2). This result supports the results from the independent sample t-test which shows that all variables rejected the null hypothesis except communication quality. This implies that all factors except communication quality were found to significantly affect students' perceived vulnerability, as per the Man-Whitney U test. Conclusively, the results from the independent sample t-test and the Man-Whitney U test shows that all variables rejected the null hypothesis except communication quality at the 95% and 99% confidence level respectively. The findings are also in line with other studies which note that students' are most vulnerable to social engineering attack, because they spend most of their time engaging with technology unrestrained and sometimes perform action carelessly (Aliyu et al., 2010; Muslah Albladi & Weir, 2019).

Recommendations

This section provides some recommendation that will help students to better understand how they can work and avoid falling victim to pretexting, a social engineering attack.

First, never trust messages that attaches monetary benefits, rewards or recognition which is to be claimed within a specified time or requires you to motivate friends/family before you can claim. This is because claiming the benefits often require the individual to click on embedded links in messages/emails which can contain malware. This recommendation is based on research findings in Tables 2 and 3. According to Ofusori and Subramaniam (2021), when you receive messages from third parties or other major institution; never click on embedded URLs in the in the email.

Second, never respond to alarming emails/messages that requires a sense of urgency relating to account verification even if it comes from a source that looks genuine or the sender looks familiar or from a known person outside the organization. This study recommends that authorized and trusted channels should be used to verify the legitimacy of the sender's company or email address. According to Kaspersky (2021) most reputable organizations will never request personally identifiable information or account details, via email. This includes your bank, insurance company, and any organization you do business with. "If you ever receive an email requesting for any type of account information, immediately delete it and then call the organization to confirm that your account is OK" (Kaspersky, 2021, p. 1).

Third, never respond to the sender of email advertising a free antivirus software to fix an immediate problem. Corroborating this findings, Ofusori and Subramaniam (2021) argue that social engineers coax unsuspecting individual to download a free antivirus software that secretly spread spyware, which in turn penetrates the individual's devices. According to Rege et al. (2019) malware might be disguised as a free software solution which may leave the individual vulnerable to attacks. This recommendation is based on research findings in Tables 2 and 3.

Lastly, when in doubt of legitimacy of the message/email, student should contact ICT departments to make sure an email is safe to open. This recommendation is based on research findings in Tables 2 and 3. Corroborating this findings, Aiden et al. (2025) affirm that an individual is most likely to trust an email/messages when the content appears to be professional, thus making the individual vulnerable to attack. In addition, students should look out for spelling errors and grammar mistakes in the content of the email. It is better to check multiple emails than to have one phishing email compromise the system (Walker, 2016, p. 64).

Limitations and suggestions for future research

In the data analysis and results section, some students chose the "neutral" option. Such students can be considered as not been aware of the risks associated with pretexting attack which can be seen as a serious threat. Also, the representatives for this study were extracted from UKZN registered students in the IS&T department. Hence, this present study is limited to the UKZN, South Africa and cannot be generalized to all higher degree institutions of South Africa. In addition, this research study adopted a quantitative approach. It is acknowledged that mixed methods or qualitative approach could have yielded a different narrative to the study. Hence, both mixed and qualitative methods are needed to be carried out in similar studies. It will be advisable to have studies that will measure the influence of social engineering attacks and its vulnerability from the academic staff perspectives. Further research can be carried out for "Spear-Phishing" & "Whaling Phishing" to understand and identify better solutions. Also, while the study had a focus on studying communication quality and to measure trust, other relevant variables like opportunistic behaviour and commitment can also be considered in measuring trust. Lastly, the study recommends the design of controls, processes and intelligent technologies that be used to curb social engineering attacks.

CONCLUSION

This study sought to explore how Communication quality influences student's trust contributing towards students' vulnerability to social engineering attack as it relates to phishing emails among ICT students of University of technology Durban. Questionnaire data collected were analysed using both descriptive and inferential statistical methods; with parametric statistical tests (independent samples t-test) and non-parametric test (Man-Whitney U test for independent samples). An independent sample t-test was employed to establish the impact of persuasion and responses on pretexting, a social engineering attacks, based on the pre-determined factors. While the non-parametric test was conducted as complements to the independent samples t-test and sought to establish the factors influencing

students' vulnerability to social engineering attacks, where data was assumed not to be normally distributed.

Findings from descriptive analysis revealed that to a significant extent, students responded positively to the influence of communication quality as it relates to trust leading to the vulnerability of social engineering attack. These results are corroborated by findings from an independent samples t-test and a Mann-Whitney U test; all of which rejected the null hypothesis and concluded that communication quality has a positive influence on student's trust contributing towards students' vulnerability to social engineering attack. The findings are also in line with other studies which note that students' are most vulnerable to social engineering attack, because they spend most of their time engaging with technology unrestrained and sometimes perform action carelessly (Aliyu et al., 2010; Muslah Albladi & Weir, 2019).

REFERENCES

- Abdullah, Z., & Musa, R. (2014). The effect of trust and information sharing on relationship commitment in supply chain management. *Procedia-Social and Behavioral Sciences*, 130, 266-272.
- Adams, J. S., & Freedman, S. (1976). Equity theory revisited: Comments and annotated bibliography. In *Advances in experimental social psychology* (Vol. 9, pp. 43-90). Elsevier.
- Adu, E. O., Ojo, O., & Adu, K. O. (2019). Evaluation of South Africa University Lecturers Accessibility and Utilization of E-Learning Infrastructure for Teaching. EdMedia+ Innovate Learning,
- Aiden, M. K., Chhabra, S., Sabharwal, S. M., & Hameed, A. A. (2025). Social Engineering Attacks: Detection and Prevention. *Emerging Threats and Countermeasures in Cybersecurity*, 349-387.
- Alabdan, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. *Future Internet*, 12(10), 168.
- 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), 5.
- Aliyu, M., Abdallah, N. A., Lasisi, N. A., Diyar, D., & Zeki, A. M. (2010). Computer security and ethics awareness among IIUM students: An empirical study. Proceeding of the 3rd International Conference on Information and Communication Technology for the Moslem World (ICT4M) 2010,
- Alseadoon, I. M. A. (2014). *The impact of users' characteristics on their ability to detect phishing emails* [Queensland University of Technology].
- Ball, D., Coelho, P. S., & Machás, A. (2004). The role of communication and trust in explaining customer loyalty. *European journal of marketing*.
- Benavides-Astudillo, E., Silva-Ordoñez, L., Rocohano-Ramos, R., Fuertes, W., Fernández-Peña, F., Sanchez-Gordon, S., & Bastidas-Chalan, R. (2021). Analysis of Vulnerabilities Associated with Social Engineering Attacks Based on User Behavior. International Conference on Applied Technologies,
- Bhattacharjee, A., & Sanford, C. (2006). Influence processes for information technology acceptance: An elaboration likelihood model. *MIS quarterly*, 805-825.
- Broadhurst, R., Skinner, K., Sifniotis, N., Matamoros-Macias, B., & Ipsen, Y. (2018). Phishing and Cybercrime Risks in a University Student Community. *Available at SSRN 3176319*.

- Bryman, A., & Bell, E. (2011). *Business Research Methods*.
- 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*.
- Chandarman, R., & Van Niekerk, B. (2017). Students' cybersecurity awareness at a private tertiary educational institution. *African Journal of Information and Communication*, 20, 133-155.
- Conteh, N. Y. (2021). The dynamics of social engineering and cybercrime in the digital age. In *Ethical Hacking Techniques and Countermeasures for Cybercrime Prevention* (pp. 144-149). IGI Global.
- Cropanzano, R., Anthony, E. L., Daniels, S. R., & Hall, A. V. (2017). Social exchange theory: A critical review with theoretical remedies. *Academy of Management Annals*, 11(1), 479-516.
- Daniel, W. W., & Cross, C. L. (2018). *Biostatistics: a foundation for analysis in the health sciences*. Wiley.
- Garcia, T. A., Fairlie, A. M., Litt, D. M., Waldron, K. A., & Lewis, M. A. (2018). Perceived vulnerability moderates the relations between the use of protective behavioral strategies and alcohol use and consequences among high-risk young adults. *Addictive behaviors*, 81, 150-156.
- Hameed, M. A., & Arachchilage, N. A. G. (2019). On the Impact of Perceived Vulnerability in the Adoption of Information Systems Security Innovations. *arXiv preprint arXiv:1904.08229*.
- Hargie, O. (2016). *Skilled interpersonal communication: Research, theory and practice*. Routledge.
- Huo, B., Zhang, C., & Zhao, X. (2015). The effect of IT and relationship commitment on supply chain coordination: A contingency and configuration approach. *Information & management*, 52(6), 728-740.
- Information & Communication Services. (2019). *Phishing and spam awareness*. University of KwaZulu-Natal. Retrieved 13 February from https://ics.ukzn.ac.za/wp-content/uploads/2018/03/Phishing_4.pdf
- Jeong, M., & Oh, H. (2017). Business-to-business social exchange relationship beyond trust and commitment. *International Journal of Hospitality Management*, 65, 115-124.
- Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. *Educational and psychological measurement*, 30(3), 607-610.
- Lord, N. (2020). Social engineering attacks: Common techniques & how to prevent an attack. *Digital Gurdian*.
- MacFarland, T. W., & Yates, J. M. (2016). Mann-whitney u test. In *Introduction to nonparametric statistics for the biological sciences using R* (pp. 103-132). Springer.
- Mitnick, K. D., & Simon, W. L. (2003). *The art of deception: Controlling the human element of security*. John Wiley & Sons.
- Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security*, 59, 186-209.
- Mouton, F., Malan, M. M., Leenen, L., & Venter, H. S. (2014). Social engineering attack framework. 2014 Information Security for South Africa,

- Muslah Albladi, S., & Weir, G. R. (2019). A conceptual model to predict social engineering victims.
- Ofusori, L. O., & Subramaniam, P. R. (2021). The Influence of Technical and Social Factors in Mitigating Threats in a BYOD-Enabled Environment. *International Journal of Information Systems in the Service Sector (IJISSS)*, 13(1), 1-30.
- Perrin, A., & Duggan, M. (2015). *Americans' Internet access: 2000--2015*. Retrieved 28 June from <http://www.pewinternet.org/2015/06/26/americans-internet-access-2000-2015/>
- Redmond, M. V. (2015). Social exchange theory.
- Rege, A., Williams, K., & Mendlein, A. (2019). A social engineering course project for undergraduate students across multiple disciplines. 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security),
- Roy, A. B. (2025). A Review of Understanding the Social Engineering in the Context of Cybersecurity. *Unveiling Social Dynamics and Community Interaction in the Metaverse*, 357-388.
- Sharma, S., Avasthi, A., Kapoor, S. K., Keswani, B., Gupta, S., & Goyal, N. K. (2026). Psychological Dimensions of Social Engineering in Cybercrime. In *Cyber Forensic Frameworks for User-Centric Human Threat Intelligence Analysis* (pp. 119-148). IGI Global Scientific Publishing.
- Stergiou, D. (2013). Social Engineering and Influence: A Study that Examines Kevin Mitnick's Attacks through Robert Cialdini's Influence Principles. In.
- Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International journal of medical education*, 2, 53.
- Tian, C., Jensen, M. L., & Durcikova, A. (2018). Phishing Susceptibility across Industries: The Differential Impact of Influence Techniques. Proceedings of the 13th Pre-ICIS Workshop on Information Security and Privacy,
- Walker, L. E. (2016). Deception of Phishing: Studying the Techniques of Social Engineering by Analyzing Modern-day Phishing Attacks on Universities.
- Zulkurnain, A. U., Hamidy, A., Husain, A. B., & Chizari, H. (2015). Social engineering attack mitigation. *Int. J. Math. Comput. Sci*, 1(4), 188198.