UNIVERSITY OF OKLAHOMA

GRADUATE COLLEGE

THE MEMORABLE MESSAGES LEADING TO THE DECISION TO TAKE SECURE MEASURES AGAINST FINANCIAL FRAUD ATTACKS:

THE CASE OF SAUDI ARABIAN STUDENTS ABROAD

A DISSERTATION

SUBMITTED TO THE GRADUATE FACULTY

In partial fulfillment of the requirements for the

Degree of

DOCTOR OF PHILOSOPHY

BY

ASHJAN ZAILA

Norman, Oklahoma

2025

THE MEMORABLE MESSAGES LEADING TO THE DECISION TO TAKE SECURE MEASURES AGAINST FINANCIAL FRAUD ATTACKS:

THE CASE OF SAUDI ARABIAN STUDENTS ABROAD

A DISSERTATION APPROVED FOR THE
DEPARTMENT OF COMMUNICATION

BY THE COMMITTEE CONSISTING OF

Dr. Patrick Meirick, Chair

Dr. Norman Wong

Dr. Elena Bessarabova

Dr. Ryan Bisel

Dr. Angela Zhang

DEDICATION

I am deeply thankful for the strength, patience, and perseverance that Allah, the Almighty, has granted me, without any power or might of my own.

Alhamdulilah.

ACKNOWLEDGMENTS

I am profoundly grateful to my father for trusting me as I embark on this journey away from home. He understands that this path has not been easy for me, especially when it comes to the emotional challenges of being apart from my beloved little ones, my nephews Abdulaziz and Ayham. Throughout my entire PhD journey, I have struggled to articulate the most daunting aspect of it, yet he can sense the weight I carry. He once shared a profound insight with me: " إذا كان سهله كان الكل اخذها" (If it were easy, everyone would earn it.) Those words have become a source of strength, fueling my confidence and motivating me to persevere with even greater determination. I also deeply appreciate my mother's unwavering prayers, which serve as a comforting reminder of her hopes for my well-being and happiness throughout this journey abroad. Though my mother may not fully grasp the challenges that come with being a PhD student, she recognizes the emotional toll of being separated from loved ones. Her poignant advice, "اسعدي نفسك بنفسك" (Make yourself happy on your own), resonates deeply within me, becoming a mantra I turn to during moments of loneliness and doubt. I would also like to express my gratitude to my sisters and brothers, whose support has been invaluable and has manifested in countless ways throughout this phase of my life.

I also want to express my gratitude to my dissertation committee for their thoughtful guidance and support throughout this dissertation. I am particularly indebted to my advisor, Dr. Patrick Meirick, for his unwavering support from my first semester in the PhD program to completing this dissertation. He was understanding and encouraging, even when I suddenly decided to change my dissertation focus. This qualitative dissertation would not have been possible without Dr. Ryan Bisel, whose expertise and constructive feedback enhanced the quality of my work. I would also like to extend my appreciation to Dr. Elena Bessarabova; I thoroughly

enjoyed taking your social influence class, which provided me with essential knowledge that contributed to this dissertation. I'm grateful to Dr. Norman Wong for the valuable insights I gained in your Survey of Communication Campaigns class, which helped shape my research interests and inform my dissertation. I also want to thank Dr. Angela Zhang for accepting the role of outside member on my committee; your contribution was invaluable to this project. I would like to express my heartfelt gratitude to all my cohorts in the Communication Department at the University of Oklahoma, who have been incredibly supportive. I was impressed by the high quality of our cohort. We consistently looked out for one another, checking in on each other's progress as we worked toward our goals. Sharing the ups and downs of my academic journey with them was both supportive and enjoyable. Gathering qualitative data proved challenging, and I want to express my heartfelt gratitude to everyone who helped me connect with Saudi students studying abroad in Western countries. I also extend my thanks to those Saudi students who took the time to share their experiences; your valuable contributions made this possible. To my Saudi, Kuwaiti, and Omani friends during my time at the University of Oklahoma, thank you for making this journey feel like a home away from home. This academic journey was filled with support, guidance, and encouragement. I am also thankful for all the difficult moments and constructive criticism I received along the way, as they have undoubtedly improved the quality of my learning. I want to acknowledge the person who may not be mentioned here but who has played a significant role in my academic journey, both before and during this time. This achievement would not have been possible without everyone's support and encouragement. Thank you all!

Table of Contents

Dedication…… iv

Acknowledgements……..…..….. ……..……..v

Table of Contents……...……..…….. vii

List of Tables ……..……...…… x

List of Figures..……..……..…… x

Abstract……..……..…….. xi

Chapter 1: Introduction……..…..…..…….. 1

Purpose of the study…….……6

Conceptual Framework……....…8

Research Goals …… ……10

Research Questions ……...10

Significance of the Study……..……11

Assumptions ……..……12

Research Positionality……13

Scope……..……..13

The Structure of the Study ……...……14

Chapter 2: Literature Review……...…….....16

Overview…….…….…….…….16

Social Engineering Attacks Background…….……..……18

Individuals' Risky Behavior…….……..…23

Individual factors and adopting security behavior…… 28

Cultural Background and Fraud Risk……31

Saudi Students Abroad……..36

Security Awareness Through Communication……...……40

Encouraging Protective Behavior: Insights from Health Communication……..……...……..47

Memorable Messages and Behavior Change…….……53

Chapter 3: Method……..…...……..…..62

Overview……..……..62

Participation selection ……..……...……..63

Design and procedures……..…….....66

Data Analysis…….76

Validation Strategies……...…80

Chapter 4: Findings……..……..84

RQ1……..……. 86

RQ2……...……..……99

RQ3……..…….……105

RQ4……..…..……..112

Summary ……...……..…..…….114

Theme one: Interactivity in Fraud Awareness……..…….……..115

Subtheme: Interpersonal Communication (Close Others & Own)…….….116

Subtheme: Intrapersonal Communication (Protective Attitude)…….....117

Theme two: One-way communication……..…118

Chapter 5: Discussion……...……...…121

Overview……...…122

Interpretation of the Findings…….……..122

Theme One: Interactivity in Fraud Awareness…….……123

Subtheme One: Interpersonal Communication (own)…….……128

Subtheme Two: Interpersonal Communication (close others)…….130

Subtheme Three: Intrapersonal Communication (Protective Attitude)……...132

Theme Two: One-Way Communication……..136

Summary of the Findings and Interpretation……...139
Limitations……...…140
Future Research Recommendations…….141
Theoretical Implications……..144
Practical Implications……..145
Conclusion……...147
References……150
Appendix A…….204
Appendix B……..205
Appendix C……..207
Appendix D……..208
Appendix E……..209

List of Tables

Table 1. The Demographic Characteristics of Participants……...……64

Table 2. Sample Characteristics…….65

Table 3. Subthemes and Categories of Participants' Responses Regarding Fraud-related Stories……85

Table 4. Secure Actions Against Social Engineering Attacks: Checklist and Additional Participant
Strategies……87

Table 5. Subthemes and Categories of Students' Responses to Secure Practices…..……89

Table 6. Participants' Levels of Concern and Associated Narrative Insights……..…...92

Table 7. Subthemes and Categories of Participants' Sources of Concern and associated Communication forms……...……94

Table 8. Subthemes and Categories of Memorable Fraud-Related stories and associated Communication forms……..……...100

Table 9. Subthemes and Categories of memorable messages contributed to behavior change……..106

Table 10. Themes and Subthemes of memorable messages and taking secure behaviors……..113

Table 11. Interpersonal communication and Associated communication Context……...……..125

List of Figures

Figure 1…….……..…….59

ABSTRACT

Social engineering attacks (SEAs) pose significant challenges today. As attackers exploit various strategies to manipulate individuals using persuasion techniques and digital tools to deceive individuals into trusting them. These manipulation strategies are designed to exploit individual information in order to access confidential details for purposes such as stealing money or disclosing sensitive information. They encompass a range of tactics, including fraud, phishing, and vishing, which represent various methods; however, the underlying objective remains consistent. Since the success or failure of these attacks often depends on individuals' concern about the risk and secure behavior, the threats of social engineering attacks may increase among those engaging in less familiar interactions, such as international students who face language barriers, cultural differences, and unfamiliar interaction norms. International students, with a focus on Saudi students abroad in Western countries, including the United States, the United Kingdom, and Australia as a case study, represent a community navigating diverse challenges outside their home countries, yet they are often overlooked in communication studies. Using an open-ended online survey, this study employed an inductive qualitative content analysis approach to analyze participants' fraud-related stories and messages to identify whether different forms of communication affect their concerns about the SEAs' risk and behavioral responses to avoid such risk. Participants were asked to recall communication events and memorable messages, as well as report any protective behaviors they adopted to safeguard themselves against SEAs' attacks. The analysis explored whether different forms of communication, focusing on memorable messages, influenced Saudi students abroad to adopt secure behavior and become concerned about such risks. The main findings revealed that interpersonal communication with close others and firsthand experiences with scammers appeared to impact participants' concern and the risk associated with such experiences. This interactive communication involved participants sharing, talking about, or evaluating fraud-related information with others or themselves. Furthermore, the findings also found that this engagement often triggered intrapersonal reflections, such as feelings of fear of attackers exploiting advanced technology to make the attacks legitimate and influence trust in conducting online transactions. Furthermore, these emotional reactions to the prevalent attacks targeting individuals' confidential information influenced participants' decisions to adopt protective actions, reflected in their avoidance strategies and self-responsibility in financial matters and online behavior. Culture and religious values rooted in Saudi and Islamic traditions also appeared as key factors influencing participants to adopt secure behavior, as emerged from their memorable messages reflecting culture-based wisdom, which influenced the decision to adopt secure behavior against SEAs. Therefore, the findings expand understanding of message effects and protective behavior change models. These models suggest that factors such as perceived vulnerability and susceptibility to a threat motivate individuals to adopt or change behavior to avoid a threat. However, in the Saudi context, the data revealed that personally relevant as well as cultural and religious values work as motivators to adopt secure actions against fraud, particularly when the messages are interactive. Notably, the study supported the idea that factors like vicarious experiences, personal narrative,

and emotional relevance were motivating factors in shaping protective behaviors among Saudi students abroad. Furthermore, the findings maintained factors like self-efficacy and attitudes toward a secure behavior, reflecting how participants evaluated their capacity to avoid a threat and engaged in precautionary actions. Practically, this study highlights the importance of designing anti-fraud communication strategies that are culturally and religiously framed, as participants shared messages that reflected personally relevant and reflected their cultural and religious values. This is especially true for Saudi Arabian students abroad, particularly when the messages are interactive. Furthermore, prevention messages can also leverage storytelling, emphasize relatable personal experiences to enhance memorability, and influence protective behavior change. The findings contribute to the literature on international students' challenges by revealing how cultural familiarity, rather than exposure to less familiar environments, critically shapes participants' concerns and behavioral responses to avoid fraud attacks. Meaning that less familiar interactions abroad did not appear to impact fraud concerns among Saudi students in Western countries. Instead, personal and emotional narratives shared within close others' networks, firsthand experiences and intrapersonal reflection were memorable and influential. While some participants recalled media messages, authority warnings, and school instructions as memorable messages to recognize the risk associated with fraud, personal and cultural connections appeared more effective in motivating protective behavior change. Furthermore, the findings illustrate how participants' fraud-related stories involving interactive communication events not only influenced their concerns about fraud risk and proactive behavior to protect themselves from the attacks but also enhanced the memorability of such interactions. The study's findings provide valuable insights into the influential forms of communication that shape risk concerns and encourage the adoption of secure behavior against SEAs. Additionally, this study maps out the behavioral changes that participants adopted to protect themselves against fraud threats. These behavioral changes captured both technical and interpersonal strategies, including password management and privacy control. The study also identifies the memorable messages feature in relation to the communication context that increased the memorability of such messages, influencing these behavioral shifts. The current study findings expand the boundaries of the messages' effect and protective behavior change of the factors associated with adopting or changing behavior to avoid a threat, particularly in the Saudi Arabian context. Furthermore, the study findings provide recommendations for improving fraud prevention communication strategies targeting international students and individuals specifically from collectivist cultures such as Saudi Arabia, suggesting that culturally framed and personally relevant messages can be more effective than solely informational appeals.

Keywords: Social Engineering Attacks (SEAs), fraud concern, secure behavior, Saudi students abroad, communication forms, memorable messages, interactive communication.

CHAPTER 1: INTRODUCTION

Digital transformation is a top priority for public organizations and individuals. However, adopting digital systems also introduces inherent risks of fraud attacks, including human-based and technology-based attacks (Singh et al., 2021; Van Steen et al., 2020; Wolff, 2018). The risk of these attacks, commonly referred to as social engineering attacks (SEAs), stems from schemes that manipulate individuals through various persuasion techniques and digital tools, deceiving them into trusting the attacker. This deception results in victims unwittingly giving away confidential information, such as personal banking details, passwords, verification codes, and more (Atkins & Huang, 2013; Bullee & Junger, 2020; Mann, 2008; Vitak et al., 2018). Additionally, since SEAs frequently occur in a virtual external environment, law enforcement faces challenges in combating these attacks, particularly those misusing channel tools such as scam phone calls and fraudulent SMS messages, etc. This situation compels individuals to take protective measures to safeguard themselves from various forms of fraud (Alhasan, 2023; Brunken et al., 2023; Jakobsson & Ratkiewicz, 2006; Puram et al., 2011; Wilson et al., 2023). These security threats highlight the need to understand how individuals' secure behavior has changed in their efforts to protect themselves against these threats (Alyahya & Weir, 2021; Alhasan, 2023; Digital Fraud, 2023; Kirova & Baumöl, 2018).

Recently, social engineering risks targeting individual users have significantly increased due to sophisticated schemes to exploit people's interaction with computers, message interpretation, and system vulnerabilities (Cranor & Garfinkel, 2005; Drake et al., 2006; Kumaraguru et al., 2007; Schneier, 2000). In response to these risks, several studies have found that individuals' impulsive behavior, trust, mistakes, and cultural factors are significantly related to fraud loss (Aivazpour & Rao, 2018; Anderson & Agarwal, 2010; Alhasan, 2023; Warkentin &

Willison, 2009). These findings highlight the necessity of exploring fraud-related stories to understand how individuals navigate less familiar interactions and mitigate potential threats, focusing on whether different forms of communication influenced their concerns about SEA and encouraged safer behavior. To do so, the study explores a diverse sample of Saudi students studying abroad in Western countries, including the United States, the United Kingdom, and Australia, providing insights into their fraud-related stories and whether communication forms influence their security behaviors against such attacks. The selection of Saudi students as a group exemplifies a population navigating new cultures, languages, and unfamiliar social interaction systems.

Given the unique context of Saudi Arabian culture, social interactions, and trust in others, these characteristics have increased the vulnerability of the Saudi people to scam threats, particularly in less familiar interactions abroad (Al-Ghaith, 2015; Alyahya & Weir, 2021). Given that the cultural influences and social interaction norms in Saudi Arabia reflect behaviors characterized by trust in others and knowledge sharing (Alhasan, 2023; Alyahya & Weir, 2021). As a result, Saudi students studying abroad may be more vulnerable to fraudulent schemes and information theft, particularly through social engineering, due to their less familiarity with foreign cultural norms, communication barriers, and social interaction practices. Furthermore, since Islamic principles deeply influence financial practices—including the prohibition of riba or exploitative gain or interest charged on loans (Siddiqi, 2004)—experiencing fraud can carry a social stigma of irresponsibility, which may discourage individuals from reporting such an incident, ultimately reducing the risk of targeting others. Concerning navigating a new culture, several studies have indicated that international students face multiple challenges in environments outside their home countries (Andrade, 2006; Baklashova & Kazakov, 2016).

Similarly, Saudi students studying in Western countries often encounter cultural, social, and academic difficulties (Alsanea, 2023). More importantly, international students who are less familiar with the local financial system, social interaction norms, cultural practices, legal regulations, and communication standards in new environments are more likely to encounter a variety of challenges, including becoming victims of fraudulent attacks. This security issue underscores another challenge Saudi students face in less familiar interactions. Thus, the qualitative inquiry explores the gap in the literature in messages and communication impact on behavior change against a threat, in the case of a fraud attack threat, especially among individuals navigating less familiar interactions or dealing with less familiar local systems away from their home country. To do so, the current study focuses on identifying the influential communication forms, i.e., messages and communication events, that impact their secure behavior in less familiar interactions.

Furthermore, human factors in fraud avoidance have become increasingly critical, and these have been shown to be significantly different across various cultures, individuals' trust levels, and individuals' impulsive behavior (Alhasan, 2023; Aivazpour & Rao, 2018; Cheshire et al., 2010). Mahanta and Maringanti (2023) note that social engineering attacks exploit human vulnerabilities by creating a sense of urgency, fostering trust, and instilling fear in potential victims instead of targeting technical flaws. These fraud schemes demonstrate how individuals in less familiar environments, particularly those adjusting to a new culture, may face heightened risks, including social engineering attacks. Their lack of familiarity with local social norms, systems, and language barriers exacerbates these vulnerabilities. Building on this background, the current study aims to extend insightful knowledge regarding whether the communication forms influence secure behavior adoption by examining qualitative insights from an individual's

memorable messages and communication events that shape secure behavior, especially in less familiar interactions, such as those experienced by students abroad. Additionally, few studies have focused on human interaction fraud, namely impersonating authority identities to steal money and the recent surge of sophisticated attacks that people face globally (Gaydos, 2023; G, 2023; Scown, 2019). Thus, Saudi students abroad provide a valuable case study to explore how diverse forms of communication influenced them to take secure behavior against fraud attacks in less familiar environments, along with cultural and religious factors that may shape their secure behavior (e.g., the prohibition of riba and trust in others).

Furthermore, unlike relying on anti-virus programs and strong passwords for protection against technological attacks (Anderson & Agarwal, 2010), avoiding human-interaction attacks can be more complicated and requires individuals to be mentally engaged and attentive, i.e., through cognitive reflection (Frederick, 2005; Kahneman & Frederick, 2005). In the context of security behavior, cognitive reflection refers to the individual's ability to make an immediate decision to avoid an attack, particularly when dealing with human-interaction-based risk. Tjostheim (2022) argues that an individual's cognitive reflection is a valuable tool to test the likelihood of a person's susceptibility to fraud attacks, focusing on phishing online attacks. Therefore, the current study explores memorable communication events and messages that resonate with Saudi students, influencing their concerns and adopting secure behavior against SEAs. Building on previous studies suggesting that messaging can foster behavioral change and shape attitudes (Glanz et al., 2008; Hornik & Kelly, 2007), research indicates that exposure to risk-related information may influence and alter behavior, particularly within prevention strategies that have primarily been explored in health-related contexts (Abdurahimovna, 2023; Noar & Zimmerman, 2005; Wakefield et al., 2010). In this regard, memorable messages (Knapp

et al., 1981) suggest the role of messages to encourage individuals to internalize the importance of protective measures, motivating them to act against a threat, which could also inform the development of effective intervention messages (Noar, 2006; Slater, 1997).

To gain a deeper insight, the current study followed the framework of Memorable Messages introduced by Knapp et al. (1981), which describes influential communication elements (e.g., advice, guidance, words of wisdom, and so forth) that significantly impact an individual's life. The ToMM provides a vital framework for exploring verbal message content and roles within the communication discipline (Cooke-Jackson & Rubinsky, 2017; Steimel, 2013). Recognizing that memorable messages are highly effective in altering an individual's behaviors by clearly conveying information and creating an emotional connection with individuals, these messages often utilize storytelling, emotional appeal, and personal relevance, making them more impactful and memorable (Kreuter et al., 2007).

Therefore, the study adopted an inductive, qualitative content analysis approach to design an open-ended survey using the memorable messages as a conceptual framework, which is justified by the need to explore whether any form of communication influenced Saudi students studying abroad to adopt protective behavior against financial fraud. Furthermore, the study explored whether individuals—as a crucial aspect to avoid financial fraud—have taken specific actions, which must be conceptualized for practical implications in mitigating sophisticated fraud-related threats tailored to Saudi students abroad and similar collectivist cultures. In addition, extends the work on the growing research on communication and behavior change about the messages that promote the adoption of protective actions against fraud, especially when individuals are navigating less familiar interactions. In this regard, according to Alhasan (2023), cultural background and level of trust significantly shape individuals' cybersecurity

behaviors, necessitating prevention materials tailored to these differences to influence behavior change effectively. Hence, the present study explores how the framework of memorable messages related to fraud prevention can illuminate potential links between taking protective behaviors and memorable messages experienced by Saudi students abroad. By examining the patterns in memorable messages from Saudi students—such as their source, content, and structure—this study seeks to identify how messages and communication events shape fraud concerns and behavior change. Qualitatively identifying these aspects will offer valuable insights into creating culturally and contextually relevant prevention messages against SEAs. Additionally, the findings of this study can contribute to the development of risk communication strategies at different levels, including institutional communication and academic literature, as well as the role of communication events in influencing individuals' concerns and adopting secure behavior against SEAs.

Purpose of the study

Exploring forms of communication, with a focus on memorable messages that promote secure behavior against social engineering attacks, represents a relatively new and underexplored area within communication studies. Still, it is crucial to examine the connection between an individual's memorable messages and their concern encouraging the adoption of secure behaviors against SEAs, specifically focusing on Saudi students studying in Western countries who encounter less familiar interaction norms in new cultural environments. Memorable messages have been found to be effective in changing an individual's behaviors, particularly emphasized in health-related messages warning people about risky practices and diseases (Anderson et al., 2020; Cooke-Jackson & Rubinsky, 2021, 2023). Therefore, the present study extends these prior works to explore whether forms of communication in relation to the

memorable messages the Saudi students abroad carry with them led them to adopt protective behavior against fraud attacks in unfamiliar environments.

Previous work emphasized the various challenges faced by international students, particularly those from Saudi Arabia, in Western developed countries (Akanwa, 2015; Causadias, 2020; Leonard, 2022; Mills, 2021). These challenges include cultural differences, language barriers, and financial issues, all of which negatively impact students both academically and socially. Furthermore, given the prevalence of SEAs targeting individual users, Saudi students abroad are at a high risk of becoming victims of fraud, which heightens the need to adopt secure behaviors to safeguard their information. While previous research has concentrated on examining fraud prevention strategies that can raise awareness among the general population, particularly older adults and local citizens, there is a lack of research addressing more diverse demographics, such as expatriates and the international community, who may be more susceptible to fraud attacks due to less familiarity with local financial systems, communication barriers, and limited access to anti-fraud resources (AlSulaimi, 2022; Blythe & Coventry, 2018; Parsons et al., 2014).

The problem addressed in the current qualitative exploratory inquiry is that Saudi students studying abroad, who are accustomed to familiar social practices and financial systems, may encounter difficulties understanding the norms of foreign interactions and financial systems when attending overseas universities. This situation could heighten their vulnerability to complex fraud attacks. Consequently, this qualitative study aimed to explore the lived experiences of Saudi students as they navigated less familiar interactions abroad to avoid social engineering attacks. It primarily focused on identifying the various forms of communication—such as impactful media messages, training programs, interpersonal communication, and mass media—that influenced their concerns about SEAs and led to decisions to take protective measures

against complex fraud schemes, including both human interaction and technology-based financial fraud in unfamiliar settings.

Conceptual Framework

The current study structure was based on the relationship between three key concepts: forms of communication, memorable messages, and behavioral change. Although the qualitative work and model on behavioral change to prevent social engineering attacks are somewhat limited, various communication and persuasion frameworks offer valuable insights into how individuals process and understand a threat, including the Health Belief Model (HBM) and the Protection Motivation Theory (PMT) (Champion & Skinner, 2008; Maddux & Rogers, 1983; Rogers, 1975). These serve as a valuable background for understanding behavior change by examining how individuals assess perceived threats and benefits, making it particularly useful for analyzing responses to fraud risks. Furthermore, according to financial literacy and behavior studies, perceived susceptibility to financial risks and the perceived severity of those risks can significantly impact individuals' financial behaviors (Lusardi & Mitchell, 2014; Mandell & Klein, 2009). For example, students who recognize the potentially severe consequences of identity theft may be more attentive in monitoring their financial settings and practicing secure behavior against fraud attacks.

On top of that, the memorable messages framework, introduced by Knapp et al. (1981), constructs the influence of individuals' memorable messages on their protective behavior, especially those from significant others. According to Knapp et al. (1981), Memorable messages refer to verbal messages that an individual receives that may affect the individual's life, such as guiding decisions and behaviors. The main idea of the memorable message's framework is that certain words or advice communicated in specific situations, e.g., from peers and family

members, can have a profound and long-term influence on individuals' decision-making and behavior. Further, several studies extend the significance of messages through interpersonal communication to include media messages in promoting behavior change and highlight the necessity for strategically designed risk communication to foster such changes (Anderson et al., 2020; Ogata Jones et al., 2006; Smith et al., 2009). These also have highlighted the message characteristics that increase its memorability, as prior studies using PMT, for instance, Van Bavel et al. (2019) found that coping messages and threat appeals encouraged the participants to engage in secure behaviors; however, the coping message—e.g., practical steps to avoid risk attempts—was particularly effective in prompting users to take action against cybersecurity threats. On the other hand, the threat appeal alone—e.g., focusing on the negative consequences of not adopting secure behavior—was less effective than when participants were exposed to both strategies, i.e., coping messages and threat appeals. Furthermore, several factors also play a role in protection behavior adoption, including peer influences and personal norms, which have been found to mediate the link between coping appraisal—e.g., online behavior, securing a home computer, and password choices—and security behavior (Mwagwabi & Jiow, 2021). Additionally, social expectations and adherence to Islamic principles, particularly in financial sittings, are deeply tied to Saudi culture and have also been found to influence Saudi citizens' behavior change (Ahmed, 2021; Mathkur, 2019; Siddiqi, 2004). Based on that background, the research questions were developed to extend the work and identify whether forms of communication and particular types of memorable messages encouraged Saudi Arabian students studying abroad to adopt secure behaviors. The selection of memorable messages frameworks was meaningful for this inquiry to identify the students' memorable messages and memorable

communication events that shaped their fraud concern and their adoption of secure practices to avoid fraud attacks.

Research Goals

The following goals guided the development of the research data collection tool, i.e., the open-ended survey, and ensured alignment with the research goal while analyzing the participants' responses.

First, Explore the participants' secure practices based on the security expert's recommendations and/or the participants' own secure behavior.

Second: Uncover the participants' level of concern about social engineers' risk in less familiar interactions and communication forms that contributed to their risk concern.

Third: Meaning-making of messages, interactions, words of wisdom, or phrases that contributed to participants changing their behavior against social engineering attacks.

Fourth: Identifying the features of the memorable message and/or interaction in relation to Saudi culture, Islamic religion, and the content and sources that influenced their concerns and adopting secure behavior against social engineering attacks.

Research Questions

Based on these goals, the research questions below addressed the purpose of this study, which was to identify and establish the connection between forms of communication, memorable messages, and adopting secure actions against social engineering attacks among Saudi students aboard.

RQ1: What behavioral change did Saudi Arabian students abroad take to protect themselves from social engineers' attacks?

RQ2: What forms of communication encouraged Saudi Arabian students abroad to take secure behavior to protect themselves from SEAs?

RQ3: In what ways did a key message (e.g., cultural, religious, content, sources) influence Saudi students to adopt protective behavior against SEAs in unfamiliar environments?

RQ4: In what ways are memorable messages and taking secure behaviors linked among Saudi students abroad?

Significance of the Study

Social engineering attacks are becoming increasingly sophisticated and leverage technical gaps and individuals' psychological vulnerabilities (Hadnagy, 2010; Thomas, 2002). These attacks are particularly threatening among individuals navigating less familiar interactions, with a focus on Saudi students abroad as a case study who are used to a culture characterized by trust and knowledge sharing, increasing their vulnerability to such attacks away from their home country (Alyahya & Weir, 2021; Alhasan, 2023). Additionally, Saudi students studying abroad come from a unique culture and social dynamics that influence their behaviors, particularly in approaching finances (Siddiqi, 2004). Furthermore, international students adjusting to new cultures might be faced with several challenges, including language barriers, cultural differences, and new interaction norms, all of which increase the susceptibility to information security threats (Alsanea, 2023; Abdel Razek, 2012; Akanwa, 2015; Bassey, 2024). Thus, the current study contributes to the growing body of research on communication and behavioral change by exploring the connection between the forms of communication and memorable messages that influenced Saudi students abroad to protect themselves against social engineering attacks in less familiar interactions.

The first contribution is to identify the kind of memorable messages related to the fraud

threat that has led Saudi students abroad to change their behavior in approaching finance or online behavior. Furthermore, the second contribution in the present study aims to explore the sort of behavioral change the Saudi Arabian students abroad took to protect themselves from financial fraud attacks, which also might highlight aspects such as the individual's trust in digital technology or reducing reliance on online/phone financial services infrastructure. The study findings are expected to contribute practical implications regarding risk communication strategies, particularly memorable messages, to promote the adoption of secure behaviors against fraud attacks in collectivist cultures like Saudi Arabia and students abroad in particular, where social practices and highly interactive relationships are emphasized (Hofstede, 2001; Long, 2005). Further, the study findings are expected to explore and explain the connection between forms of communication and memorable messages influencing the individuals' concern about SEAs leading to the adoption of secure practices. These implications will be helpful to prevention message designers, future studies assessing individuals' anti-fraud awareness, and policymakers aiming to develop more effective fraud prevention campaigns. Additionally, the findings can support organizations in designing training programs that leverage the study's concepts and themes of forms of communication in relation to memorable messages to enhance anti-fraud awareness and foster a culture of security. In conclusion, the critical part of the current study is finding the pattern regarding the influential communication materials for adopting protective behavior and raising the individual's security awareness against financial fraud among Saudi Arabian students.

Assumptions

Saudi students pursue their education in various countries worldwide. The researcher selected Western countries, as they are among the most preferred destinations for Saudi students

(see Appendix B). The researcher designed an open-ended survey that asked the participants to recall fraud-related incidents. It is assumed that using the *cognitive prompt technique* and a closed-ended question in the form of " Do you remember?" followed by the open-ended question of "What?" has facilitated accurate and meaningful data collection. The study assumed that giving participants the option to respond in their preferred language, i.e., Arabic or English, offered them more flexibility to express their thoughts. The study assumed that intentionally selecting participants based on predetermined criteria, including adopting secure actions to protect their information, would yield valuable insights for the survey question, reflecting unique and purposive selection. The study employed strategies for validation, and the data analysis was conducted as objectively as possible to minimize any bias. The study assumed the findings broadly reflect the larger population of students from the chosen groups, namely, Saudi students enrolled in Western countries.

Research Positionality

As a Saudi researcher, I have firsthand insight into the cultural and social dynamics that shape Saudi interactions with technology and perceptions of security threats. My familiarity with the local context, including the high value placed on social influences and the rapid adoption of communication technologies, directly informs my research objectives and methodological choices. This positionality enables me to interpret and translate the participants' inputs. However, I maintained a critical distance to ensure that the study setting and interpretation were inductive in the participants' data rather than my assumptions. The validity of the research setting, findings, and interpretations was achieved through the qualitative strategies discussed in the methodology section.

Scope

The study is geographically scoped to Saudi students studying abroad in Western countries, including the United States, the United Kingdom, and Australia. Furthermore, other Saudi students study abroad and enroll in different countries, such as East Asia or South America, for data gathering, which might yield more robust findings. The study focused on a particular set of cultural groups and may not represent all cultural groups. The study used a specific sample criterion to include only participants who took secure actions to protect themselves from social engineering attacks. This criterion has limited the data gathered to include only the data relevant to the study questions, offering more meaningful and valuable findings. The study was focused on collecting qualitative data and did not include quantitative data such as statistical measures and numerical assessments. As such, the study prioritized qualitative data such as fraud-related incidents, messages, and stories; only two closed-ended questions were analyzed related to the participants' secure actions and their level of concern. Furthermore, participants who did not provide answers to any of the free-response questions were excluded from the analysis; these questions contributed meaningful insight and relevant data to the study's goals. The time window in which the researcher collected the data from the study's population was limited, reflecting the amount of information needed for the study. As part of the study's scope, the questionnaire was only distributed via email, so the participants primarily included participants who regularly check their email; this may exclude students who may prefer to complete the survey in other forms.

The Structure of the Study

Several studies indicate that individuals in Saudi Arabia are increasingly exposed to anti-fraud messages through various channels, including face-to-face interactions and media exposure. These messages aim to educate and raise awareness about fraud prevention (Alyahya

& Weir, 2021; Almuhammadi & Alsaleh, 2017; Alanezi, 2016). Therefore, they highlight the importance of communication in promoting secure behaviors among Saudi users. Consequently, the current study examines whether a form of communication with a focus on memorable messages, words, and events has influenced Saudi Arabian students abroad to alter their behavior to safeguard themselves against financial fraud. Identifying the relationship between forms of communication and protective behavior change enhances understanding of risk communication strategies and effective prevention messaging. The dissertation is divided into five chapters. The introductory chapter lays a foundation for the rest of the dissertation by addressing the issue of information security threats and highlighting Saudi users' behavior concerning the risks of social engineering attacks directed at individuals. It also outlines the study's key concepts, methods, population, and study scope. The second chapter offers a literature review on the topic to develop the research questions, exploring previous studies on social engineering threats, behavioral changes, Saudi culture, and other relevant areas pertaining to these threats and protective behavior. The third chapter discusses the research methodology, covering design, data collection, instrument development, and data analysis. It also describes the measures employed to ensure the data's validity and trustworthiness. The fourth chapter presents the study findings by addressing the research questions and using tables to illustrate the data's categories, sub-themes, and themes. The fifth chapter discusses the findings and their interpretation, provides the findings' implications for the field of communication and future research, and examines the significance of these findings and their practical contributions. Following the study limitations, chapter five also draws conclusions based on the overall findings and suggests directions for future research. The last section of the dissertation presents the appendixes and offers additional information, including the survey and statistical data.

CHAPTER 2: LITERATURE REVIEW

Overview

Globally, social engineering attacks (SEAs) have become a major threat as they increasingly exploit technical gaps and individuals' psychological vulnerabilities (Alotaibi et al., 2016; Heim, 2023; Hadnagy, 2010; Thomas, 2002). This threat primarily lies in the strategies employed by attackers, misusing advanced technology and channel tools, as well as exploiting human cognitive vulnerabilities and emotional reactions, making preventive actions essential. (Baror & Venter, 2019; Zhuang et al., 2015). Similar to technology-based attack strategies that exploit software gaps, human-based strategies leverage sophisticated performances to convince individuals to disclose sensitive information or take actions that compromise their security. This threat highlights the critical importance of exploring the factors and individuals' lived experiences in recognizing social engineers' actions (Caudle, 1990; Hadnagy & Kelly, 2014). Several studies predominantly assert that individual behavior plays a crucial role in avoiding and preventing social engineering attacks (Alhasan, 2023; Ceesay et al., 2018; Schneier, 2000). Therefore, it is valuable to explore the factors related to whether forms of communication, particularly received messages, contributed to fraud concerns, encouraging secure practices to protect confidential information.

This qualitative study explores whether forms of communication in relation to memorable messages (Knapp et al., 1981)—as distinct and impactful interactions—encouraged Saudi students abroad in Western countries to take secure behaviors to protect themselves against SEAs. The current qualitative research aimed to explore the fraud-related stories and messages among Saudi students studying in Western countries; a community group may be particularly vulnerable due to cultural, language, and interaction norms differences. Given that this study was among the few to investigate whether forms of communication influence fraud concerns and

taking secure behavior adaptation against SEA within the field, it closely references studies that analyze memorable messages as a framework (Kaufmann et al., 2021; Knapp et al., 1981) alongside with research examining how individuals' security information awareness and cultural backgrounds affect their responses to attacks (Alhasan, 2023; Almrezeq et al., 2021). Furthermore, given that the selected population of Saudi students studying abroad, the current study closely aligns with prior research examining the challenges faced by international students pursuing education in foreign countries. Building on this foundation, the present exploration extends the focus to determine the communication forms that influenced these students in addressing challenges in protecting confidential information (Abdel Razek, 2012; Alraddadi, 2015; Davis, 2014; Lefdahl-Davis & Perrone-McGovern, 2015). Furthermore, while previous studies predominantly adopted quantitative methods, several also utilized qualitative approaches to explore the experiences of Saudi students abroad. However, a need remains further to investigate the lived experiences of Saudi students abroad to identify the communication events influencing secure behavior to protect oneself from social engineering attacks.

In the current chapter, the researcher reviewed several aspects of the literature to comprehend the link between communication forms and the adaptation of secure behavior against social engineering attacks and cybercrimes in general. It begins with the definitions, types, and techniques of social engineering attacks, followed by an exploration of individuals' risky behaviors, individual factors, and the adoption of security behaviors, as well as the experiences of Saudi students abroad. The current section also introduces the role of interpersonal and mass communication in enhancing security awareness, insights on protective behavior from health communication, the memorable messages framework in behavioral interventions, and Saudi Arabia's cultural and social factors influencing its security threats.

Furthermore, the current section explains the relevance of Saudi students as a demographic, considering that Saudi students studying in the US, UK, and Australia represent a significant and under-researched population in the context of secure behavior against social engineering attacks. Exploring whether forms of communication effectively improved the Saudi students' security practices abroad might improve the strategies for the protection of other vulnerable populations, e.g., international students and communities in less familiar environments.

Literature Review

Social Engineering Attacks Background

The terms fraud, scam, and social engineering attacks generally refer to the risks in cybersecurity attacks that target individuals' and businesses' valuable information (Chargo, 2018). The current study's scope focuses on attacks that encompass attempts at unauthorized access and the theft of sensitive information for stealing money and information purposes, specifically using language and communication to trick individuals into disclosing confidential information (Baror & Venter, 2019; Zhuang et al., 2015). Because the study focused on international students' secure behavior against social engineers who are often less familiar with the natural language abroad, i.e., English, and local interaction norms, i.e., communication patterns, away from their home country, focus on Saudi students abroad as a community group, this research has found that social engineering attacks are significantly the biggest threat to their information security (Akanwa, 2015; Gonzalez, 2024; Marginson, 2012; *Simulated Phishing Update*, 2024). To address the problem of this study, the paper identifies several views of social engineering attacks. This encompasses several distinct meanings contingent upon the context, all of which refer to the action of obtaining unauthorized access to victims' confidential information for illegitimate reasons (Hinson, 2008; Hatfield, 2018; Oxford English Dictionary, 2023). One,

according to the Oxford English Dictionary (2023), social engineering is *"The use of deception in order to induce a person to divulge private information, or esp. unwittingly provide unauthorized access to a computer system or network."* Second, several studies have referred to (SEAs) as a type of action that depends on hackers' social skills to persuade individuals to comply with a request (Mitnick & Simon, 2003; Ramamoorti, 2008). Others also describe social engineering or simply call it fraud as a combination of psychological tricks with hacking skills to intentionally obtain unfair advantages or harm others (Bonini & Boraschi-Diaz, 2013; Cohen & Felson, 1979). For example, Rieber (2024) emphasized that social engineering encompasses the use of persuasive strategies and interpersonal interactions designed to deceive individuals into disclosing confidential information.

Historically speaking, the concept of social engineering began to be shaped by the phenomenon of "*phone phreaking*" from the late 1950s through the early 1970s (Chadd, 2020; Hinson, 2008). This started when individuals discovered vulnerabilities in the telecommunications system, allowing them to manipulate the network signals to make free long-distance calls. This "*phone phreaking*" phenomenon has since highlighted the technological and human manipulation techniques foundational to breaking actions without authorization, referred to as *phreaking* or hacking (Brush, 2014; Coleman, 2012; Kumar, 2022). In light of the diverse terminology employed to articulate the idea behind SEAs, several studies concur that applying this concept involves a strategy for acquiring unauthorized access that leverages technical gaps and/or individuals' psychological vulnerabilities (Hadnagy, 2010; Thomas, 2002). That is, fraudsters, according to Maurer 1999, said that fraud "*never remain stationary; the principle may be old, but the external forms are always changing"*(p. 55) Explain that all forms of fraud are widely considered one of the most significant threats to information security, as fraudsters refine

their schemes over time by leveraging the development of technology and other means (Steinmetz et al., 2020; Talib & Rusly, 2015). This indicates that fraudsters consistently advance their strategies to exploit new vulnerabilities and circumstances, thereby enabling them to remain ahead of detection measures. For instance, during the COVID-19 pandemic, fraudsters rapidly found opportunities to exploit the widespread fear and uncertainty among the public, which not only upon public health concerns but also extended to identity theft, insurance fraud, and online payment schemes (Kennedy et al., 2021; Ma & McKinnon, 2021; Zhang et al., 2022). During that period, the American Federal Trade Commission raised concerns about the deceptive advertisements on social media platforms, which falsely claimed to offer pandemic-related health solutions and protective equipment (Levine, 2021). Based on this background, in the current study, the previous definitions of social engineering pertain to one or more individuals influencing the behaviors of others, which is a context deemed applicable in the realm of human interactions and communication. Therefore, for the current analysis of secure behavior adaptation, the terms in the current study interchangeably refer to social engineering attacks as any actions of scams, fraud, or hacking to describe the actions of fraudsters targeting individuals' information. This information could be specific, including credit card details, social security information, and sensitive information.

Thus far, studies examining social engineering attacks have classified these attacks as predominantly employing two essential vectors: the technological-based and human-interaction approach (Atkins & Huang, 2013; Peltier, 2006). While in both approaches, scammers intentionally aim to deceive and manipulate individuals into divulging confidential information or performing actions, each approach uses different malicious techniques to gain their intent (Abraham & Chenr-Smith, 2010; Huang & Brockman, 2011; Mann, 2017). First, technological-

based, or so-called cyberattacks, utilize computer systems' weaknesses or digital technology to gain unauthorized access to personal or organizational systems (Hatfield, 2018; Rahman, 2020). These cyberattacks use various malicious actions such as malware, viruses, phishing, false websites, emails, spoofing, and hacking of computer programs. These actions exploit software vulnerabilities for unauthorized information, such as stealing credit card details, damaging operations, or personal revenge against an organization's network or individual users' systems (Gulati, 2003; Halder & Jaishankar, 2011; Moore, 2014). Continuously, cybercrime carried out through digital technology rapidly advances their attacks by leveraging different platforms or paths, forcing comprehensive public awareness in relation to that (Button & Cross, 2017; Elnaim, 2013; Nickerson, 2019).

The second is the human-interaction approach, which relies on deception through human interaction; these attacks are performed through actions such as impersonation. For instance, receiving a call from someone posing as an IT support representative, fellow employee, or third party who intends to gain the victim's trust and obtain unauthorized access to sensitive information (Gulati, 2003). Impersonation is typically one of the most used ways social engineers use to obtain the information they need, particularly considering the advanced technology tools allow scammers to falsify their caller ID as displayed by an official authority, which is referred to as spoofing caller ID (*Caller ID Spoofing*, 2024). They use the sophisticated tactics of spoofing ID to make the calls appear legitimate and convincing (McNicholas & Smith Randolph, 2024). This has been recently reported in the U.S. across several states. For example, scammers impersonate dead police officers to steal money from unsuspecting victims and claim they own fines or warrants (Dalli, 2023; Gaydos, 2023).

Overall, SEAs employ a diverse range of sophisticated technologies that can be

remarkably inventive, enabling them to avoid security detection systems, especially when such attacks are aimed at an organization's critical information (Atkins & Huang, 2013). Thus, it has been noted that a considerable number of fraudulent attacks are directed toward organizational entities, frequently leading to the compromise of individuals' personal information (Davinson & Sillence, 2010; Milletary & US Center, 2007; Moore & Clayton, 2007). Consequently, these attacks can expose users' data, such as names, addresses, and financial details, facilitating the scammer's schemes to reach and persuade users to disclose more information, such as passwords and verification codes. Despite differences in the techniques of social engineers to conduct such attacks, the ultimate purpose remains the same (Alhasan, 2023). One of the common techniques the hackers use is the psychological manipulation technique, which is mainly used in non-technical social engineer attacks, i.e., human interaction-based attacks approach (Baror & Venter, 2019; Chargo, 2018), which was the primary key in the current study to explore how Saudi students abroad were able to comprehend the threats associated with SEAa and adopt secure practices to protect themselves from such attacks during their journey abroad.

These psychological techniques rely on the use of natural language and other communication forms to manipulate *the would-be-target/object*, misusing channel tools such as phone calls and text messages (Baror & Venter, 2019; Zhuang et al., 2015). For example, several studies investigating social engineering tactics have emphasized the role of the emotional appeal technique as a motivator for individuals to engage in action, with fraudsters exploiting and persuading victims to grant access to victims' financial information (Cooney & Gazzaniga, 2003; Messick & Bazerman, 1996). Social engineers have strategies to exploit individuals' weaknesses by invoking emotions related to the victims' situations, such as fear, urgency, or excitement, encouraging victims to disclose financial or confidential information (Atkins & Huang, 2013;

Michel & King, 2019; Workman, 2008). This way of manipulating individual emotions has been discussed using the metaphor of the "*Bad Apple,"* which serves to highlight the manner in which scammers exploit the emotional and cognitive processes of victims, thereby redirecting victims' attention and persuading them to act against their best interests (Härtel & Panipucci, 2007; Lewin, 2015). These cognitive biases can produce automatic emotional responses, allowing social engineers to gain access without identifying themselves (Tversky & Kahneman, 1974; Zajonc, 1968). Certainly, the significant threats of social engineering attacks are mainly their ability to use language and social skills to exploit the individual's emotional state and cognitive biases to disclose personal information or to commit the attacks (Raman, 2008; Thompson, 2006; Workman, 2008). This far, a number of these persuasion techniques to attack individuals have been recognized by researchers, such as *choice-supportive bias*, *exposure effect*, and *anchoring* (Raman, 2008); these techniques have been varied and become more creative depending on the hacker and the technology used (Manske, 2000).

Individuals' Risky Behavior

Since individuals are at significant risk of falling prey to social engineering attacks, their secure behavior is key in mitigating and preventing such attacks (Alhasan, 2023; Ceesay et al., 2018; Schneier, 2000). Wilson et al. (2023) found that the success of scams significantly relies upon the actions of victims who frequently disclose personal information and neglect the law warning of scammers' tactics, concluding that most fraud schemes would not succeed without the victims' cooperation (Wilson et al., 2023). Consequently, individuals' precautionary or protective measures encompass taking physical steps to safeguard personal information, updating software, employing robust passwords, and ignoring unknown calls, all of which are essential. To illustrate, several sources have noted that fraudulent activities, including false technical support

and other scam tactics, primarily ask individuals to confirm personal information or engage with unsecured websites that can compromise login credentials, which emphasizes the necessity of adopting secure practices (Brody et al., 2007; Holtfreter et al., 2008; Kshetri, 2010). Similarly, Vitak et al. (2018) further highlighted the importance of individuals developing a sense of security and privacy when sharing sensitive information, acquiring the necessary skills to conduct online transactions safely, and the ability to detect fraud attempts. Although various digital tools have been developed to warn users about potential attacks on insecure websites, there has been limited focus on human-based attack approaches. For instance, lottery scams, job offer scams, and phishing calls often involve fraudsters impersonating legitimate representatives to convince victims to share confidential information (Hadnagy, 2010; Krebs, 2014). Considering that social engineers frequently have strategies to reach and exploit their target victims, leveraging psychological biases and human tendencies, such activities target *the would-be-target/object* (Baror & Venter, 2019; Zhuang et al., 2015), who may be more vulnerable, including members of foreign communities, international students, and people in financial need (*The psychology of social engineering, 2020*).

Considering the importance of individual behavior in avoiding fraud attempts, the current qualitative study explores whether communication events in particularly memorable messages led individuals, i.e., Saudi students in Western countries, to adopt secure behavior to protect themselves from social engineering attacks in less familiar interactions. In the case of Saudi security practices, several studies have found that Saudi citizen's expectation that the government is responsible for information security, as well as the tribal culture and trust in others, were among the factors negatively influencing Saudi users' security information in their home country (Alarifi et al., 2012; Alzubaidi, 2021; Alyahya & Weir, 2021). These factors

collectively hinder Saudi citizens' tendency to adopt security practices, leaving them vulnerable to attacks and threats on social engineers.

Governmental and non-governmental organizations worldwide have made substantial efforts to increase public awareness regarding preventing fraud attacks and to educate the public about identifying and preventing SEAs and fraud attacks in general, particularly within educational institutions (Heim, 2023; Mousa, 2019). These initiatives aimed to improve cybersecurity awareness and reduce fraud threats through training programs and workshops in schools and universities regarding such attacks. Further efforts were implemented through other strategies, including authority announcements, public campaigns, and cybersecurity detection systems specifically designed to counter such attacks (Alhasan, 2023; Heim, 2023; Mutune, 2021). These aim to inform individuals about various fraud tactics, encouraging them to adopt secure practices. In the current study, Saudi participants were expected to be exposed to such anti-attack initiatives and various educational media messages, raising their concern about fraud. Additionally, several studies have shown that other negative experiences with fraud faced by family members and peers can motivate individuals to adopt secure behaviors (Rader et al., 2012; Redmiles et al., 2016). Thus, in addition to exploring the communication forms and messages influencing fraud's concern and secure practices, this part identifies the behavioral changes Saudi participants made to safeguard their information and determine their secure practice patterns. Hence, exploring the behavioral outcomes provided a road map to the patterns of secure practices, offering insight into memorable communication events that resonate with the target demographic, i.e., Saudi students abroad. Moreover, examining the behavioral changes in the study served the study's goals to ensure that the findings would be relevant and accurate to the intended group.

The following research question served as a guiding framework for communication and behavioral outcomes exploration.

> **RQ1:** What behavioral change did Saudi Arabian students abroad take to protect themselves from social engineers' attacks?

In line with this, research conducted by Alyahya and Weir (2021) identified a direct correlation between the intentions of Saudi users to respond to phishing emails and the factors of attitudes, subjective norms, and perceptions of behavioral control, as introduced by the theory of planned behavior (Fishbein & Ajzen, 1975). These factors have increased Saudi users' tendency to respond to harmful and malicious emails in their familiar interactions, i.e., in the Saudi Arabian environment (Alyahya & Weir, 2021). The current research expands the scope to explore the behavioral change the Saudi students took to navigating less familiar interactions while studying in Western countries, e.g., professional environments, daily life, and online interaction. Regarding the Saudi citizens' security behavior, Alyahya and Weir (2021) emphasized developing security programs to reduce the susceptibility to social engineering attacks among Saudi users. Additionally, alongside individuals' cautious behaviors, technology-based detection mechanisms, such as website tools and user-friendly interfaces, have been found to play a critical role in enhancing and guiding users' security. These tools provide explicit warnings and assist individuals in identifying phishing attempts and forcing storing passwords, thereby guiding their secure practices. For instance, Dhamija and Tygar (2005) and Ye and Sean (2002) have developed a prototype "*trusted paths*" for web browsers to help users verify secure connections to trusted sites. Furthermore, several web browser toolbars offer safety indicators, such as red or green lights, to notify users of potential risks (Wu et al., 2006; Zhang et al., 2007).

Nonetheless, individuals' understanding and digital skills in noticing phishing attempts are essential to the efficacy of anti-attack technology detection (Kumaraguru et al., 2007).

Several studies have highlighted that the effectiveness of technology-based systems, including cybersecurity tools such as antivirus software, is predominantly contingent upon user behavior and attitudes toward cyberattack risks (Bada et al., 2019; Parsons et al., 2014). Consequently, errors such as not adhering to guidelines or non-compliance with secure practices by users these behaviors were referred to by Stanton et al. (2005) as *naïve mistakes,* which often undermine the reliability of technological detection systems (Liginlal et al., 2009; Parsons et al. 2013). In this context, where user fraud awareness is critical for the security and efficacy of cybersecurity technologies, Ceesay et al. (2018) evaluated the institutional approach to information systems security, revealing challenges associated with adopting a unified strategy. Hence, a comprehensive sociotechnical systems (STS) approach was proposed to integrate technological components and promote secure cybersecurity behaviors.

This approach incorporates high-reliability techniques, fosters a safety culture, and enhances the understanding of fraudulent tactics. This was also found in Food fraud studies, which have shown that comprehensive approaches involving technology, regulatory oversight, and public awareness are necessary to enhance individuals' ability to reduce their susceptibility to deceptive practices (Yiannaka, 2023). Further, a study by Schneier (2000) highlighted that one of the critical vulnerabilities in preventing fraud lies in the human factor. To further support the idea of comprehensive approaches, scammers use persuasive tactics, requiring technology countermeasures and concurrently educating users on detecting fraudulent language (Emigh, 2007; Puram et al., 2011; Visa's Stay Secure, 2023). Therefore, the Saudi efforts to prevent the spread of fraud among individuals extend beyond technology detection. Hence, The Saudi Central Bank, or so-called SAMA, also issued warnings about digital fraud early in 2022,

advising users to be cautious with their data and to verify the legitimacy of websites (*Saudi Counter-Fraud Framework,* 2022).

Individual Factors and Adopting Security Behavior

A significant body of research has examined the factors influencing individuals' decisions to adopt and use security measures against fraud, particularly among individuals who are not experts in security as well as home users. These studies predominantly focused on the elements that impact individual's decisions to implement security systems and tools (Alanazi et al., 2022; Anderson & Agarwal, 2010; Bada et al., 2019; Lee & Kozar, 2005). While security information and protective measures are now readily accessible to individuals, the process of making security decisions in response to threats varies significantly among users (Anderson & Agarwal, 2010; Kumar et al., 2008; Kirova & Baumöl, 2018; Zurko, 2005). Despite the abundance of security advice available from various sources (Redmiles et al., 2016; Rader et al., 2012) and widespread belief in the efficacy of security measures (Wash & Rader, 2015), research suggests that individual factors, including cultural background, personal beliefs, and interaction norms, play a moderating role in shaping adoption of these behaviors (Alhasan, 2023; Alsaif, M. 2014; Alanazi et al., 2022). These factors may highlight why individuals do not always implement security practices despite their perceived effectiveness.

Previously, in this paper, we touched upon the fact that individuals respond to messages differently, which has been observed across various topics of interest in relation to security warnings and educating the public. According to Wash and Rader (2015), educating users on securing their home computers should not emphasize the quantity of security knowledge, as "*not all users should receive the same messages"* (p. 309). In this regard, they examined and revealed that an individual demographic aligns with their belief in the effectiveness of protective

measures, i.e., antivirus software, combined with their belief that they are unlikely to be a potential scam target; these factors often challenge the successful communication of protective measures. This means that tailoring security information to the different demographic segments might be more effective than providing a "*one-size-fits-all*" (p. 320) education approach (Wash & Rader, 2015).

Other studies revealed that the more significant the sense of ownership individuals feel for their devices, the higher their intentions to protect them. In alignment with that, several studies have indicated that users' concern for their information privacy significantly influences their intention to adopt secure systems against online attacks (Gurung & Raja, 2016; Kumar et al., 2008; Stern & Salb, 2015). For example, users with greater privacy concerns value their information not being shared and abused, particularly online transactions. This influences their decision to disclose personal information and their intention to provide their information online (Dinev & Hart, 2006; Hong et al., 2021). Similarly, prior studies have argued that impulsive behavior, where individuals act without fully considering the negative consequences of sharing sensitive data or clicking on unknown links, increases the individual susceptibility to risky online activities (Aivazpour & Rao, 2018; Cheshire et al., 2010).

In addition, the impact of a message varies among individuals, and it is influenced by factors such as the recipient's security beliefs, self-efficacy, socioeconomic status, and, most importantly, familiarity with fraud activities (Hargittai, 2007; Redmiles et al., 2016). For Saudi students abroad, exposure to less familiar interactions might increase their susceptibility to SEA risks, particularly making the effectiveness of anti-fraud messages critical. For example, students abroad may recognize phishing scams due to familiarity with their home country's local system, local language, and other authority transaction practices. However, the same experience may

differ when dealing with less familiar practices in foreign systems. Therefore, exploring the fraud-related story behind the students abroad engaging with and responding to various interactions while protecting themselves from financial attacks can provide valuable insights into developing risk communication strategies for fraud prevention by investigating the factors that influence their secure behavior in foreign environments.

Notably, the role of psychological characteristics in adopting security behavior, e.g., using antivirus software, choosing strong passwords, or software updates, cannot be ignored. These characteristics were proposed by Kumar et al.(2008), who aimed to find ways to increase the non-expert user's adoption of security protection technologies. They found that computer anxiety significantly negatively impacted users' awareness of the availability of security measures such as anti-virus as well as their attitude toward using technology protections such as firewalls. Building on that, it has been observed that users' awareness and knowledge of attack threats are not sufficient to adopt security-related behavior, and neither can be precisely defined or measured due to individual differences in nature (Lee & Kozar, 2005; Moustafa & Maurushat, 2021; Schrader & Lawless, 2004). For instance, AlSulaimi (2022) and Furnell et al. (2007) both found that despite respondents' confidence in their awareness of threats and the use of safeguards, significant gaps in knowledge and understanding exist. Additionally, Furnell et al. (2007) revealed that knowledge gaps are evident not only among novice users but also among those with advanced computing experience.

Additionally, Pervaiz et al. (2019) emphasized the importance of experienced individuals guiding new users to avoid SMS scams. The research showed that new users are especially vulnerable to SMS fraud due to their lack of awareness regarding the dangers of receiving spam messages from unfamiliar sources. According to Pervaiz et al. (2019), vulnerability is especially

prevalent among marginalized and rural communities. Nevertheless, urban residents who might be educated, such as older adults and women, are also at risk of being scammed because they are unaware of sophisticated attacks attempting to steal banking details or credentials (Pervaiz et al., 2019), as are international students who may face heightened vulnerability to scams despite being educated. Additionally, several studies have revealed the common misconception that older and less educated people are the primary fraud targets; in fact, the actual characteristics of fraud victims are found to be younger and of higher education levels (Kerley & Copes, 2002; Rebovich et al., 2000; Titus et al., 1995). Like the urban residents in the study by Pervaiz et al. (2019), Saudi students abroad may be less familiar with the local financial system or sophisticated fraud attacks, making them susceptible to attacks on their banking and confidential information. Concerning the security practices and the potential of communicated messages to enhance individual such practices, this emphasizes the importance of exploring anti-fraud-related messages, words, and narratives from the lens of students abroad lived experience, particularly given the considerable cultural adjustments and language barriers these foreign students face. It situates the focus on exploring the study problem through the population perspective as a case study, often allowing the researcher to uncover practical insights regarding social realities, specifically about the challenges for international students in Western countries, including language and cultural barriers. Thus, less familiarity with the local systems in a new culture can increase the student's risk of falling victim to fraud, necessitating effective risk messages to enhance awareness and prompt preventive actions.

Cultural Background and Fraud Risk

Cultural and social norms as dimension factors influencing individual behavior and attitudes have been a valuable lens for understanding SEA risk, which is essential for

understanding how communication can resonate with individuals' vulnerabilities and integrate deterrent and preventive measures to combat social engineering attacks effectively (Albrecht et al., 2012; Getie Mihret, 2014). In the current study, the Saudi Arabian cultural values and social interaction norms aspects were introduced due to their impact on Saudi individuals' cybercrime threats and risks in both human interaction and technology-based schemes (Almrezeq et al., 2021; Zayid & Farah, 2017). In the current secure behavior scope, culture is defined as the shared beliefs, values, and attitudes that shape the individual's decision-making and behavior (Geertz, 2008), particularly influencing Saudi people's interactions and technology usage. Culture also includes *"that complex whole which includes knowledge, belief, art, morals, law, custom, and any other capabilities and habits acquired by man as a member of society"* (p.1) (Tylor, 1871). Others, like Hofstede (1980), described culture as the collective values and practices that shape and distinguish a group of people from other groups. These definitions perspective provide a lens on how current cultural norms and individual practices might make people more vulnerable to social engineering attacks than others. In other words, hackers can exploit the communicative dimension of cultural trust, which influences individuals' behavior toward digital use and interactions (Alhasan, 2023; Hofstede, 2001).

To illustrate, several studies emphasize that Saudi citizens' social interaction norms are characterized by interactivity and trust in others, making them susceptible to particular vulnerabilities, including responses to fraudulent schemes (Al-Ghaith, 2015; Alyahya & Weir, 2021). For example, studies have shown that participants are more likely to respond to fraudulent emails when these emails employ social proof strategies (Alqasa et al., 2014; Cialdini, 2007). According to previous studies, social proof refers to individuals' tendency to rely on the opinions and guidance of others when making decisions. This particular behavior was evident among

Saudi citizens, who exhibited a heightened tendency to respond to phishing emails and were influenced by social cues beyond close family and friends, such as clicking on links in trending social media notifications or acting on provided feedback (Alyahya & Weir, 2021). Trust in other individuals is also fundamental to many cultural backgrounds, including Saudi Arabian culture. This cultural trait influences individual behaviors, such as trusting authority figures, decision-making, and knowledge sharing (Mayer et al., 1995). Considering authority trust, Alyahya and Weir (2021) investigated how social engineering persuasion techniques—Authority, Social Proof, and Scarcity—influence Saudi user's responses to phishing attacks. Their findings revealed that cultural influences, particularly when using authority themes, in which emails mimic government officials, affect the intentions to respond, given the high trust in authority figures. The influence of social proof and scarcity also highlighted the role of subjective norms that shaped Saudi users' intention to respond rapidly to phishing attacks.

These insights are critical for exploring Saudi students, considering them to be more susceptible to fraud tactics away from their home country, and which communication strategies impacted them to become more secure against fraud. Another factor found by Getie Mihret (2014) is that cultures with high power distance, in which people in that culture give great deference to others, such as authorities, have higher levels of fraud risk exposure. This finding was also highlighted across diverse cultural groups, which showed a high level of trust in others, government, and/or business leaders significantly influence individuals' risk perceptions and security behaviors (Alhasan, 2023; Alyahya & Weir, 2021; Mayer et al., 1995). Notably, trust in business leaders increases Saudi citizens' vulnerabilities to security risks (Alhasan, 2023). This, in fact, was one of the social engineers' strategies to exploit this trust by using schemes such as the authority email strategy. For example, scammers send emails that expertly mimic ministry

themes and logos, fostering a sense of credibility and prompting recipients to trust and respond to the emails (Tashkandi, 2021).

Thus, this highlights the influence of certain Saudi cultural norms, as people tend to enjoy socializing through interaction with others, making decisions based on others' guidance, and exchanging opinions and feedback via social media (Alsanea, 2023; Alyahya & Weir, 2021). By examining the prior studies, the review highlights the high-risk Saudi users face within their familiar environment and demonstrates the need to focus on exploring what influenced Saudi students abroad to protect themselves from fraud attempts in less familiar environments. Furthermore, the current study emphasizes the role of widespread anti-fraud knowledge circulating between individuals through personal interaction or mass media (Rainie et al., 2013; Redmiles et al., 2016). However, more studies need to explore which forms of communication in relation to memorable messages most encouraged Saudi students abroad to recognize the risk associated with fraud and adopt secure practices against those threats.

Furthermore, the Islamic religion has a significant influence on Saudi culture, including those around financial practices like *riba* (exploitative gain or interest), which is forbidden under Islamic law (Siddiqi, 2004). Given the deep roots of Islamic principles in Saudi society, which greatly shape the attitudes toward financial activities, experiencing financial fraud can be socially seen as an indicator of irresponsibility, contributing to the potential stigma of individuals who fall victim to scams. In other words, in Saudi Arabia, fraud victims may experience the shame and social stigma of not being able to protect their finances within a society that promotes ethical and Islamic behavior. In light of this, examining Saudi students abroad can reveal how exposure to different social interactions and financial systems affects their fraud awareness, contributing to a broader understanding of effective communication strategies against fraud.

Considering the interactive nature of Saudi Arabian people, it has been observed that a variety of fraudulent methods spread lies in human interaction and gaining individual trust, which mostly leads to significant financial and identity losses. These social engineering attacks encompasses unauthorized investment opportunities, fake online job offers, and deceptive financial aid claims. (Al-Ghadhori, 2023; @SaudiChannelOne, 2022; Yemeni, 2023). Thus, the Saudi cultural context necessitates a deeper investigation into the kinds of messages and factors that can promote protective behaviors against fraud, considering Saudi individuals victimized by fraud may hesitate to reveal their experiences due to fear of the social stigma of ignoring Islamic teachings and naiveté. Therefore, understanding Saudi Arabia's culture in financial practices is critical for fraud prevention strategies, considering the stigma associated with fraud victims, which could play a social barrier to combat fraud, involving not warning others and avoiding reporting it to authorized sources.

In Saudi Arabia, social influence, particularly subjective norms, has been linked to security behaviors, where Saudi users were influenced by societal pressures and feedback provided by family, peers, and community regarding online safety practices (Alyahya & Weir, 2021; Alotaibi et al., 2016). This has also been explored by Anderson and Agarwal (2010), who found that social influence in the form of subjective and descriptive norms positively influenced users' intentions to comply with security behavior, i.e., protecting their own devices. Likewise, the descriptive norms described in secure-related behavior refer to the user's beliefs on what other people do to enhance their security, e.g., "*if I see others doing it, I will be more inclined to do it myself*" (p. 621), as an essential consideration in individuals' secure behavior (Lee & Kozar 2005; Rivis & Sheeran, 2003) Furthermore, the subjective norms addressed in the Anderson and Agarwal (2010) study refer to what individuals believe about what others think/expect he/she

should do, which also found to be significant component affecting the individual's intention to comply with security guidelines (Lee & Larsen, 2009), however, conflicted results exist (Lee & Kozar 2005).

Despite increasing efforts to measure Saudi Arabian's awareness of fraud, there is limited research to explore the communication events, particularly messages that effectively raise public recognition of fraud risk and how these measures translate into behavioral changes (e.g., AlSulaimi, 2022; Almrezeq, 2021; Alanezi, 2016; Alzubaidi, 2021). Given the significant gap in understanding message sources and themes that influenced individuals' fraud concerns and behavior regarding fraud risk in Saudi Arabia, focusing on Saudi students abroad is particularly relevant. The relevance of Saudi students abroad as a valuable sample is highlighted by their diverse communication contexts and fraud risks in less familiar cultures. The findings will contribute to determining effective risk communication strategies for fraud prevention, which can be critical for local and expatriate communities in navigating financial transactions.

Saudi Students Abroad

Currently, a significant number of Saudi students are pursuing higher education abroad, with the United States, the United Kingdom, and Australia being among the top destinations. Therefore, these Western countries were selected for the current study. Meanwhile, in the U.S., nearly 17,000 Saudi students are enrolled, the UK hosts around 16,000 Saudi students, and Australia has approximately 4,000 Saudi students (Ministry of Education, Saudi Arabia, n.d.). Several studies have found that international students encounter a range of challenges in environments outside their home countries (Andrade, 2006; Baklashova & Kazakov, 2016). Similarly, Saudi students pursuing their educations in Western countries often confront challenges due to cultural, social, and academic differences (Alsanea, 2023). Alsanea (2023)

found that language barriers and differences in American cultural norms, such as gender relations and social dynamics, contributed to social isolation among Saudi students in the United States despite the generally warm welcome they received from Americans. By addressing these issues, Saudi students in the U.S and other Western countries may increase their vulnerability to social engineering attacks as they are less familiar with the interactions norms in new environment.

The current study, based on the prior studies, revealed that often Saudi students in Western universities face various challenges (Alsanea, 2023; Hofer, 2009; Heyn, 2013), and given that more Saudi students continue to study abroad, they might be at risk to deal with the sophisticated cyber threats and social engineering attacks. These challenges often arise during interactions across different cultures and social settings, increasing their susceptibility to fraudulent schemes such as phishing emails and fake job offers. The review identifies areas where existing research has explored aspects of Saudi students studying in Western countries related to their socio-political attitudes and engagement, as well as students' self-efficacy at U.S. universities (Abdel Razek, 2012; Alraddadi, 2015). For example, several studies have examined Saudi students' adjustment challenges, particularly faced by Saudi women studying abroad. Their experiences highlighted these with expectations versus reality, experiences of discrimination, and navigating cultural changes (Davis, 2014; Lefdahl-Davis & Perrone-McGovern, 2015). However, despite these valuable insights exploring such experiences abroad, limited research has focused on Saudi students' security behaviors, particularly concerning whether forms of communication motivated them to adopt secure behaviors against SEAs and scams in general during their less familiar interactions with norms abroad. Furthermore, this gap suggests the need for further exploration into which and how Saudi’s cultural and social interaction norms, e.g., trust, influenced their vulnerability to such attacks.

Regarding college students' security practices, the King Abdulaziz Center has studied domestic Saudi university students for National Dialogue to assess their awareness of fraud attacks, and it was found that 62% of respondents reported encountering financial fraud attempts through phone or other channel tools. Furthermore, 53% of the participants stated that the fraud negatively impacted their lifestyle and family life, 16% mentioned it disrupted their saving plans, and 31% had to abandon specific purchases (*62% of Saudis Exposed to Attempts, 2022*). Furthermore, the Naif Arab University of Security Sciences (NAUSS) has documented a significant increase in online financial fraud actions, emphasizing criminals' various tactics to deceive individuals (*Saudi University Issues Warning, 2022*; SAMA Launches First Edition, *2023*). To illustrate, these tactics include creating fake versions of government apps and websites, with approximately 14,000 recorded downloads of these fake applications, as well as over 137,000 Arabs visit fraudulent financial websites daily and are exposed to diverse fraud strategies. The NAUSS also found that fraudsters impersonate bank employees to deceive victims into updating personal data and providing one-time passwords to access individual bank accounts.

More recently, AlSulaimi (2022) assessed Saudi citizens' awareness and protection methods against cyber threats. The study found that while most had not experienced cyber threats, they used various protection methods and security practices, with automatic antivirus updates commonly used. However, the study participants who self-reported as well-educated internet users via smartphones and private networks expressed concern over future threats and emphasized the need for shared responsibility, particularly from the government, to combat fraud. Considering this, students studying abroad in Western countries and dealing with less familiar interaction systems are at higher risk of becoming fraud victims, most of which cause

financial losses. Therefore, it is crucial to conceptualize whether forms of communication contributed to raising the concern about fraud and educating them to adopt secure behavior against fraud attacks, particularly considering their potential exposure to anti-fraud materials through personal experiences, mass media, anti-fraud natural efforts, and security alerts.

In addition to the fact that SEAs are widespread globally (Nickerson, 2019) and Saudi citizens have shown a tendency to respond to phishing emails (Almrezeq, 2021; Alyahya & Weir, 2021), they are at high risk of falling victim to sophisticated fraud attacks. Thus, exploring which factors encourage them to protect themselves against social engineering attacks outside Saudi Arabia's familiar environment can help design targeted support messages to ensure Saudi students' success and well-being while studying abroad. Furthermore, exploring and analyzing participants' responses, wherein they expressed their fraud-related stories, can enhance our understanding of the memorable and influential materials associated with memorable messages and communication events. This is particularly relevant to the concepts of memorable messages that significantly influenced students abroad to adopt more secure practices. Given that several studies have examined foreign students' challenges abroad, the current study broadens this work to investigate Saudi students' secure overseas behavior and identify whether communication events have encouraged participants to adopt that behavior. The following research question was developed to determine whether forms of communication have influenced Saudi students abroad in Western countries to take secure behavior to protect their information from fraud attacks.

> **RQ2:** What forms of communication prompted Saudi Arabian students abroad to take secure behavior to protect themselves from SEA?

Saudi students studying abroad may encounter various challenges, including language barriers, new cultures, and less familiar interactions. Therefore, it is crucial for students abroad better to understand local interaction norms and the financial systems, as they notably rely on online

communication, particularly when engaging in financial transactions (Andrade, 2006; Choudaha & Schulmann, 2014; Marginson, 2012). Accordingly, the current study emphasizes the need to understand if memorable communication events are associated with adopting secure behaviors while navigating such interactions. The research aimed to identify effective strategies for fostering security awareness and behavioral change by exploring the communication types and messages that motivated Saudi students to adopt protective practices. Synthesizing the prior studies, the review within the broader context of fraud prevention and Saudi users' recognition of fraud highlighted the study's focus. Further, the review identified areas where existing research is limited, particularly regarding Saudi students abroad and their unique vulnerabilities to fraud risk in less familiar environments.

Security Awareness Through Communication

The effectiveness of communication messages in promoting secure behaviors is still debated, emphasizing the need to identify whether forms of communication events influenced individuals' fraud concerns and secure practices. Nevertheless, the growing awareness of the threats associated with social engineering attacks has resulted in heightened efforts to prevent and mitigate these attacks. Given that social engineer attacks rely on human interactions, such as scam calls, attackers manipulate their *the would-be-target/object* using emotional appeals and cognitive strategies to persuade them to disclose sensitive information (Baror & Venter, 2019; Cooney & Gazzaniga, 2003; Zhuang et al., 2015). Several studies argue that technology detection tools alone are insufficient in addressing the threat of SEAs, emphasizing the importance of enhancing users' awareness of the tactics employed in these attacks (Almrezeq et al., 2021; Alhasan, 2023; Elnaim, 2013). Further, many studies have highlighted that raising individuals' recognition of fraud is essential for mitigating these threats (Kim et al., 2021; Mouton et al., 2016; Visa's Stay Secure,

2023). Hence, globally, government and private institutions have utilized media channels to launch educational campaigns aimed at enhancing fraud detection. Examples include ENISA's cybersecurity awareness campaigns in Europe and Interpol's global initiative to combat online fraud. In Saudi Arabia, notable efforts have been undertaken to implement advanced technological security systems for detecting fraudulent activities alongside educational initiatives designed to empower individuals to protect themselves, particularly against fraud involving human interaction techniques (Abdullah et al., 2021; Alyahya & Weir, 2021; Elnaim, 2013; *Saudi banks launch campaign*, 2022).

Contrasting perspectives on the efficiency of security education emerge in recent literature, with Kumaraguru et al. (2007) contending that standard security notifications are largely ineffective in imparting knowledge to individuals about phishing attacks. Kumaraguru et al. (2007) compared standard email security notices with embedded training models to educate users about phishing during regular email use. Their findings revealed that training materials formats in texts, graphics, and comic strips significantly improved users' ability to recognize phishing threats, highlighting the limitations of standard notices. This research is particularly relevant to the current study's focus on individuals with limited expertise in scam detection. Kumaraguru et al. (2007) also emphasized principles for message design, including integrating training into users' routines, using clear and concise messages, and providing actionable guidance to enhance protective behaviors. These principles will be pivotal in evaluating participants' responses and enhancing the efficacy of the intervention messages against SEAs. They suggested that users may struggle to recollect anti-scam messages from e-commerce entities and government bodies, as these messages often lack clarity and fail to address real-world issues. This implies that individuals may have difficulty comprehending the risks associated with standard email security messages.

Conversely, Wash and Cooper (2018) discovered that security education and training serve as effective means to modify end-user security behaviors. Their research emphasizes that users can enhance their technological knowledge and improve their ability to identify fraudulent activities. In accordance with the study participants, Wash and Cooper (2018) determined that the facts and advice presented by a security professional were more efficacious than stories provided by a peer. The findings indicate that implementing security expert techniques can assist users in making more secure decisions to mitigate the risk of fraudulent activities. This is consistent with the conclusions drawn by Davidson and Sillence (2010), who emphasized that providing risk warning information alone can heighten awareness, fostering intention and behavioral changes. For the current study, intervention studies offer evidence on strategies for preventing fraud, highlighting their limitations and successes. For example, Kumaraguru et al. (2007) found that standard security notices are ineffective, suggesting the need for more precise and simple communication. Wash and Cooper (2018) argue that security education and training can improve user behavior and help detect fraud attempts. These studies highlight best practices and gaps in current anti-scam strategies, offering valuable insights to guide future research and enhance fraud prevention communication strategies.

Moreover, incorporating shared experiences into communication strategies is crucial for increasing engagement and trust, thereby improving the effectiveness of fraud prevention efforts. For instance, Andrews and Boyle (2008) investigated how communication sources shape individuals' perceived risk and behavioral responses in online transactions, highlighting the significance of tailored communication in influencing secure behaviors. The previous study demonstrated that interpersonal communication significantly influences individuals' use of online platforms, particularly for transactional purposes such as online purchasing. Andrews and Boyle (2008) emphasized that social interactions, including discussions with family and friends, are

pivotal sources of information shaping individuals' attitudes toward new technology and innovation. This aligns with Rogers' (1995) theory of diffusion of innovations, suggesting the importance of interpersonal interaction in adopting new technologies. Furthermore, Andrews and Boyle (2008) also identified mass communication strategies' impact on shaping individuals' perceptions of credit card fraud and online purchasing behavior, including fear-based campaigns, fraud horror stories, and media warnings. Further studies have found the significant role of face-to-face peer support groups for fraud victims, emphasizing the necessity for increased peer support in the recovery process, given that fraud victims may not only experience financial losses but also have them affect their physical health and emotional state (Cross, 2019; Redmiles et al., 2016).

Furthermore, the review highlights that the effectiveness of prevention materials against fraud attacks is still a topic of debate, with several studies reporting positive outcomes, such as anti-phishing training programs that have proven effective in enhancing user security awareness (Dodge et al., 2007; Kumaraguru et al., 2007). Similarly, Blythe and Coventry (2018) examined the factors influencing employee anti-phishing behaviors, emphasizing the importance of effective training programs. In contrast, researchers like Davinson and Sillence (2010) found no impact of the training program on encouraging users to adopt secure online behavior. Additional researchers were doubtful about the effectiveness of the anti-fraud campaigns and argued that they had hardly any impact on users (Bada et al., 2019; Ceesay et al.,2018). For instance, Ceesay et al., 2018 claimed that human error is a significant contributor to information system losses and training alone is insufficient, reporting that "*enterprises that do not have awareness training are doing 12% better than those that have training programs*" (Ceesay et al., 2018, p.3). Similarly, Bada et al. (2019) analyzed why cyber security awareness campaigns often fail to influence user behavior, emphasizing the importance of designing more effective and targeted interventions.

In light of the inconsistent results, it is evident that individual differences in processing various types of messages or information related to fraud prevention—such as educational messages, fear/threat messages, and awareness training—play a significant role in determining the success or failure of fraud prevention interventions. These differences highlight the importance of tailoring communication strategies to effectively address diverse audiences and enhance the effectiveness of intervention materials (Bullee & Junger, 2020; D'Andrea et al., 2022). Additionally, it has been observed that SEA strategies are continuously evolving, leveraging technological advancements and exploiting uncertain circumstances, which makes recognizing scams increasingly challenging for individuals (Işık et al., 2024; Shen & Stringhini, 2019).

In Saudi Arabia, Alotaibi et al. (2016) pointed out that the rapid expansion of communication technologies and internet usage has increased cybercrime, with many participants unaware of the associated threats. Despite having good IT knowledge, they revealed that participants needed more awareness of cybercrime threats and cybersecurity practices (Alotaibi et al. 2016). The study emphasized the necessity of a comprehensive model to improve cybersecurity awareness, with most respondents expressing a preference for using the applications-based approach. A recent study has shown a notable increase in cybersecurity awareness among the participants (Almrezeq et al., 2021). Despite this, Almrezeq et al. (2021) revealed that many students who fell victim to cybercrimes chose not to report these incidents to local authorities, suggesting that gaps remain in their understanding of how to address fraudulent attacks. This emphasized the need for more public content on cybercrime prevention and guidance on addressing such issues within the framework of Saudi local laws. Considering the prior findings, the current study highlights the vulnerability of Saudi students abroad to SEAs, primarily stemming from their less familiarity with local systems and interaction norms, these gaps are often

exploited by fraudsters through targeted scams. Overall, despite the insights provided by these studies, the authors acknowledged certain limitations in developing a comprehensive model for anti-fraud awareness and protection practices for Saudi Arabia residents (Alotaibi et al., 2016; AlSulaimi, 2022; Almrezeq et al., 2021). Furthermore, the risk of SEAs targeting students studying abroad remains a significant concern, as they are particularly prime targets for scammers due to their varying abilities to communicate effectively and navigate financial matters compared to local students. Common scams include job scams, Visa fraud, and impersonation by fake immigration authorities (G, 2023; Scown, 2019)

In a global context, the Australia Parliament House of Representatives Standing Committee on Communications (2010) emphasized that many internet users often lack awareness of cybersecurity threats. This was attributed to insufficient educational initiatives, the complexity of public policy responses, and inadequate online safety measures that failed to alert general users to sophisticated attacks effectively. Accordingly, several studies highlighted the critical role of anti-fraud awareness materials in addressing such threats, emphasizing that fraud cannot be fully mitigated until all users develop a heightened sense of caution and awareness (Sipayung et al., 2022; Talib & Rusly, 2015; Yuniarti & Ariandi, 2017; Zahari et al., 2019). Puram et al. (2011) also emphasized the crucial role of user awareness in combating fraud threats, advocating for educational campaigns to raise consumer awareness and prevent online scams. Further, self-awareness of the risk associated with SEA relies heavily on an individual's understanding of the steps required to secure personal information and their intention to take protective actions against such threats (Hazari et al., 2008; Parsons et al., 2014; Tschakert & Ngamsuriyaroj, 2019). One significant challenge faced by students studying abroad, which heightens their vulnerability to social engineering attacks, is their lack of familiarity with the local language and terminology

associated with fraudulent activities, such as skimming, spoofing, and phishing. Accordingly, the current study explores the fraud-related incidents, including formal messages, shared stories, training programs, or personal experiences, that influenced Saudi students studying abroad fraud recognition during less familiar interactions in Western countries. Although institutions attempt to educate students through orientation programs and workshops designed to raise awareness about potential scams, linguistic and cultural barriers often limit the effectiveness of these initiatives (Gomes et al., 2014; Sawir et al., 2008).

Given the limited exploration of which forms of communication are associated to influenced students abroad to adopt secure behaviors, it is important to note that previous studies have primarily evaluated the effectiveness of training and intervention messages aimed at changing behavior in response to fraud attacks. However, these studies often focus on enhancing awareness among skilled employees rather than ordinary users. Additionally, they frequently employ pre-developed phishing attack simulations (Davinson & Sillence, 2010; Kumaraguru et al., 2007), analyze campaign materials (Chugh & Narang, 2023.; Van Steen et al., 2020), and conduct online anti-fraud knowledge assessments (Othman et al., 2015; Sipayung et al., 2022). Indeed, by examining existing studies on anti-scam communication messages, the review highlighted relevant focuses those interpersonal interactions, such as peer experiences and support groups, are vital for raising fraud recognition and enabling individuals to adopt protective practices through shared experiences (*Counter-Fraud Framework, 2022*; *Social Media Scams: Understanding, 2019*). Similarly, small group discussions and workshops have proven more effective than formal presentations in enhancing security awareness and behavior (Albrechtsen & Hovden, 2010). Nevertheless, existing literature offers valuable insights into the practical communication techniques for encouraging behavior change, identifying factors that influence users, and

highlighting materials that resonate with individuals in combating fraud threats. This knowledge contributes to developing communication strategies to communicate protective behaviors to individuals effectively. Nevertheless, further research is needed to examine whether communication events, especially memorable messages, influence the security behavior of Saudi students studying abroad and to identify the strategies that promote behavioral change. In particular, it is essential to concentrate on students studying abroad to guide fraud prevention communication strategies resonate with communities navigating less familiar interactions.

Encouraging Protective Behavior: Insights from Health Communication

Several studies have shown that communication campaigns, especially health messages, can result in behavioral changes, including increased knowledge, beliefs, or attitudes when credible sources are clear, relevant, and delivered (Abroms & Maibach, 2008; Noar, 2006; Snyder, 2007). For example, a study in the health context indicated that exposure to breast cancer messages has significantly influenced women's adoption of preventive behaviors against the disease, highlighting the role of source messages in promoting behavior change (Smith et al., 2009). Although studies on behavioral change to mitigate social engineering attacks remain relatively limited, existing communication and persuasion models offer critical insights into how individuals perceive fraud-related threats. First, The Protection Motivation Theory is widely used in health-related behavior and demonstrates the critical role of severity, susceptibility, and response efficacy in shaping individual health-protective motivations. The Protection Motivation Theory (PMT), developed by Rogers in 1975 and further elaborated by Maddux and Rogers in 1983, posits that human cognitive processes play a substantial role in shaping behavioral responses when faced with a potential health threat. The PMT suggests that individuals engage in either one of the two main appraisal processes: threat appraisal, which involves individuals' perceived severity and

vulnerability of the threat. The other approach is referred to as the coping appraisal process in which individuals believe in their ability to respond to threats (response efficacy/self-efficacy)—self-efficacy was incorporated, drawing from Bandura's (1997) research on the concepts. The coping appraisal also involves the process in which individuals perceive the cost of performing the recommended protective behavior (response cost), such as the effort and time associated with taking the coping response (Maddux and Rogers,1983; Rogers, 1975). During threat appraisal, individuals evaluate the threat's severity and their vulnerability to the risk; if they perceive the threat as highly severe and likely to affect them, it can lead to maladaptive behaviors like denial or avoidance—emotional response—i.e., fear of threat (Mwagwabi & Jiow, 2021). Otherwise, individuals will engage in coping appraisal, i.e., response efficacy, to evaluate the effectiveness of implementing protective behaviors, and self-efficacy—i.e., the confidence in performing the recommended security behaviors; in the same hand, individuals perceive the inconvenience part of performing the protection behavior, i.e., the response costs. Generally, individuals with positive coping appraisals will develop adaptive behaviors to mitigate the threat (Bandura, 1997; Maddux & Rogers, 1983).

Recently, the use of PMT applications has extended to the areas of information security and fraud threats to examine individual protection behavior against online fraud and cyberattacks (Mwagwabi et al., 2018; Thompson et al., 2017). Van Bavel et al. (2019) demonstrated that coping messages, such as practical recommendations to avoid potential risk exposure, were particularly effective in encouraging secure behaviors against cybersecurity threats. While threat appeal alone highlighting negative consequences was less impactful, combining them with coping strategies significantly enhanced participants' protective responses. Additionally, various factors, such as peer influences and personal norms, significantly impact protective behaviors. These factors

mediate the relationship between coping appraisal and overall security behavior, such as online practices, securing personal devices, and password management (Mwagwabi & Jiow 2021). Particularly, Mwagwabi and Jiow (2021) found that the perceived severity of threats and perceived susceptibility, i.e., compliance with social media security and password guidelines, were fully influenced by personal norms. In their case, teenage participants will comply with the security measures to avoid feeling ashamed if their social media accounts were hacked; in contrast, interestingly, the study found that peer influence works differently with teenagers as they might prevent compliance with the protective measure to avoid being overly cautious in front of their peers.

Expanding on these insights, the experiences of embarrassment and shame among Saudi students studying abroad remain unexplored; however, social-expectations and the strong influence of Islamic principles, especially in a financial context, are integral to Saudi cultural norms (Ahmed, 2021; Mathkur, 2019; Siddiqi, 2004). To illustrate, in Saudi society, behavioral responsibility is highly valued, and experiencing financial fraud may be perceived as a personal failure, with social stigma associated with it. Overall, this insight could be practically helpful in exploring memorable messages promoted by students abroad to encourage protective behavior in less familiar interactions, particularly where Van Bavel et al. (2019) emphasized the crucial role of coping appraisal in promoting behavior change and the significance of strategic messages, such as practical steps to avoid fraud attacks, designed for public communication. By identifying which form of communication resonates with students abroad, the study findings can provide unique strategic messages (coping messages) that encourage them to take protective behaviors to avoid fraud in less familiar environments.

Additionally, the Health Belief Model (HBM) Rosenstock (1974) provides a valuable

background for exploring behavior change by analyzing how individuals evaluate perceived threats and benefits, making it particularly useful for analyzing participants' responses to SEA risks. The HBM suggests that four components influence health-related behavior involving the individuals' susceptibility to a threat (Perceived Susceptibility), the potential consequences resulting from the threat (Perceived Severity), positive attitudes toward adopting safer practices (Perceived Benefits), lastly, the challenges the individuals perceive toward taking preventive practices (perceived barriers) (Becker & Rosenstock, 1987; Rosenstock, 1974; Rosenstock, 2005). The HBM has been widely applied in health contexts to understand how individuals make decisions about their health behaviors, such as vaccination uptake, exercise, and eating habits (Champion & Skinner, 2008). The practical aspects of the Health Belief Model regarding the threat of social engineering attacks provide insight into the factors influencing individuals' concerns about fraud and the decisions to adopt or disregard safer behaviors in response to fraud risk. For instance, some individuals might perceive secure measures against fraud as inconvenient or time-consuming, thus presenting perceived barriers to adopting such practices. Hence, the Health Belief Model (HBM) factors provide valuable guidance for crafting educational messages to enhance individuals' anti-fraud awareness, such as highlighting the positive outcomes resulting from protective actions.

Applying the Health Belief Model (HBM) to investigate factors influencing adopting protective behavior against social engineering attacks is particularly relevant for students studying abroad. For example, this means that individuals who perceive a high risk of potential attacks and recognize the benefits of taking protective measures increase their likelihood of engaging in secure practices. Research on financial literacy and behavior indicates that perceived susceptibility to financial risks and the perceived severity of those risks can significantly influence individuals'

financial behaviors (Lusardi & Mitchell, 2014; Mandell & Klein, 2009). For example, participants who recognize the severe consequences of identity theft may be more likely to monitor their financial activities and take secure behavior. Considering the HBM in the educational role of anti-fraud messages could enhance the design of effective messages by addressing the perceived barriers and benefits of adopting secure behaviors. In other words, based on the HBM cognitive constructs, it is influential to emphasize the individual's perceptions of the severity of fraud threats, susceptibility to being victimized, and perceived benefits and barriers to taking secure behaviors; such components can guide the message design to adopt safer financial practices. The HBM, as discussed by Davinson and Sillence (2010), suggests that individuals are more likely to adopt secure financial behaviors if they perceive a significant threat and believe that taking specific actions can reduce that threat. Davinson and Sillence (2014) study on user perceptions of fraud threats and secure behavior during financial transactions using technology revealed significant findings.

Despite uncovering the considerable threat of fraud, the participants generally perceived the risk as low, as many believed they were unlikely to be affected by fraud and did not consider it their responsibility to take preventive measures. Further, the conclusion of Davinson and Sillence's study points out issues surrounding user security and the difficulties in changing behavior (2014). These issues included a lack of responsibility for fraud incidents, uncertainty about behaviors designed to counteract fraud, and doubts about the potential efficacy of preventive measures. Overall, the study demanded improved educational initiatives to bridge the gap between perceived and actual threats, encouraging more protective and responsible behavior in fraud prevention. This aligns with findings from other studies that indicated that low perceived threat levels of scams contributed to insufficient preventative actions among individuals, necessitating

comprehensive awareness campaigns to raise the perceived severity and susceptibility to the sophisticated social engineering attacks (Dodge et al., 2012; Langenderfer & Shimp, 2001).

Given the significant role of user behavior in cybercrimes, it is evident that enhanced user caution could effectively prevent many fraudulent activities (Alyahya & Weir, 2021; Crossler et al., 2013). Bada et al. (2019) argue that fostering behavioral change requires more than simply providing risk-related information; it necessitates a deeper understanding of individuals' behavioral motivation and attitudinal shifts. This aligns with the Theory of Planned Behavior/Reasoned Action (TPB) by Ajzen and Fishbein (1975). The theory suggests that if an individual holds a favorable attitude towards a behavior, perceives strong social pressure to engage in it, and believes they have the capability to perform that behavior, they are more likely to form an intention to do so. Consequently, this intention increases the likelihood of engaging in the behavior (Ajzen & Fishbein, 1980; Schifter & Ajzen, 1985). Considering that the study population navigates distinct Saudi and Islamic cultural and social dynamics that shape their behaviors, particularly in financial decision-making (Alshebami, 2022; Alghamdi et al., 2021). The TPB's three components of attitudes, subjective norms (social pressure), and perceived behavioral control are highly relevant in the Saudi Arabian context, where social norms, social expectations, and Islamic principles are emphasized (Alsaif, 2014; Long, 2005; Siddiqi, 2004).

The current investigation is expected to locate cultural values, social norms, and religious attitudes to influence Saudi students abroad in fraud avoidance practices, which can be involved in effective message design tailored to the Saudi Arabian context. Further, cultural background involving individual beliefs and values has influenced human behavior and perception, particularly regarding fraud risk (Causadias, 2020; Hull et al., 2021; Warkentin & Willison, 2009). According to Alhasan (2023), individuals from various cultural backgrounds demonstrate different behaviors

and perceive different levels of trust regarding cybersecurity. Therefore, they concluded that it is important to incorporate cultural differences in designing cybersecurity messages, training, and awareness initiatives to modify individual behaviors effectively.

Memorable Messages and Behavior Change

A message in communication refers to a unit of information conveyed from one individual to another, either directly or indirectly, and processed through numerous daily interactions. Often, messages are transmitted in different forms and play a crucial role in shaping and influencing individuals' behavior across various issues (Berger & Calabrese, 1974; Berger, 2014; Fishbein & Ajzen, 1977; Petty & Cacioppo, 1986). While most of these messages may have a brief impact, certain ones hold the potential to deeply influence an individual's life, as highlighted by Knapp et al. (1981) and Ogata Jones et al. (2006). Knapp et al. (1981) introduced messages that have notable and influential impacts on people's lives, making them maintain these messages for a long time as memorable messages (MMs). Further, Knapp et al. (1981) posited that messages retain memorability when they are especially relevant to the recipient's situation and desires. Furthermore, the credibility of the message source is considered a crucial element in facilitating lasting message impressions on individuals (Knapp et al., 1981). For example, during the COVID-19 pandemic, it has been observed that the message's impact occurs when it is most evident in reducing uncertainty and fostering resilience during challenging times (Dunleavy & Yang, 2015; Kaufmann et al., 2021; Lucas & Buzzanell, 2012). Prior studies have also shown that messages are most impactful when they are emotionally positive, socially contextual, and personally relevant.

The memorable messages framework proposed by Knapp et al. (1981) provides a valuable multi-disciplinary lens to explore organizational, educational, and health studies to

address relevant issues and context for generating theories and practical implications such as assessing post-campaign effectiveness and messages motivating behavioral change (Cranmer & Myers, 2016; Merolla et al., 2017; Smith et al., 2001). For example, Anderson et al. (2020) guided their study through individuals' memorable conversations. They found the MM framework provides valuable insights into how associated sources, i.e., campaign materials, can effectively impact the intended audiences. Thus, in the context of secure behavior adoption, identifying the messages the Saudi students abroad received from various sources, e.g., relative stories, personal experience, or warning signs, in which these messages impacted them to adopt secure behavior against SEAs. This will extend another layer of identifying the potential link between memorable messages and adopting secure behavior against SEAs.

The memorable messages framework has various applications, particularly in public health studies. These applications mainly focused on exploring the messages that lead individuals to behavioral change, which effectively contributed with practical implications to designing effective intervention messages in that area (Ellis & Smith, 2004; Nazione et al., 2011; Stohl, 1986). Moreover, compelling evidence from health communication research suggests that impactful messages can profoundly influence individuals toward preventive behavior. As per the study conducted by Cooke-Jackson and Rubinsky (2023) on the contemporary status of memorable messages in communication literature, the health communication field has seen a surge in the volume of such publications since 2017. Further, it has been observed that memorable messages in health communication seem to offer theoretical and practical implications, mostly on what actually works to educate the public about an issue (Cooke-Jackson & Rubinsky., 2023; Miczo et al., 2013; Smith et al., 2010). These provide insights and offer a framework for creating compelling health messages that are more likely to be remembered and

influence individuals' health behavior. Anderson et al. (2020) analyzed 28 memorable conversations about living kidney donation and transplantation, which were initiated due to the Living Kidney Donation and Transplant (LKDT) campaign aimed at Native American communities. The results demonstrated that the campaign materials stimulated conversations and enhanced the efficacy of communication about LKDT. Based on that, it appears that there is value in examining the individual's memorable conversations as a criterion for evaluating the efficacy of related campaigns. Although the current study was not limited to exploring the efficacy of anti-fraud materials on individuals' decision to adopt secure behavior, it was expected to identify memorable public fraud-related materials within the participants' response context, which can provide valuable insight. Regarding campaign evaluation approaches, formative studies identify which communication strategies effectively enhance an individual's knowledge and shape their recognition of an issue (Coffman, 2002; Snyder et al., 2012; Willoughby & Noar., 2022). In this context, examining students' memorable communication influences their fraud concerns, leading them to adopt secure behavior, which can provide initial insights into the connection between memorable messages and the adoption of secure practices, particularly considering Saudi students' vulnerabilities in less familiar interactions.

Drawing from prior research, it was evident that specific characteristics play a significant role in the memorability of messages, which depends mainly on the issue being considered. For instance, a study by Waldron et al. (2023) delved into the impact of memorable messages on student responses to the COVID-19 pandemic. They revealed that moral messages emphasizing empathy and communal responsibility had a significant impact, especially from trusted sources like family members. The study findings maintain the Knapp et al. (1981) MMs characteristics, which emphasized the importance of source credibility, message clarity, simplicity, actionable

steps provided in response to the message, and the emotional impact—whether through fear, urgency, or empathy—in guiding protective behavior and sense-making (Cooke-Jackson & Rubinsky, 2021; Kumaraguru et al., 2007; Waldron et al., 2023). Furthermore, Wakefield et al. (2010) found that well-designed and strategically implemented public health campaign materials, particularly those targeting smoking cessation, physical activity, and nutrition, can effectively alter health behaviors. Wakefield et al. (2010) also found that messages that evoke emotional responses or provide actionable steps are more likely to yield positive behavioral outcomes.

The review identified areas where the impactful messages reflect characteristics such as message clarity, relevant topics, source credibility, and evoking emotion, which is fundamental for promoting behavior change across various contexts, including threatening phenomena like social engineering attacks. Yet, the review demonstrated the need for a focused investigation of Saudi students abroad as a vulnerable population in less familiar interactions and what memorable messages, characteristics, patterns, and themes influenced their adaptation of secure behavior. Furthermore, several studies have revealed the significant role of cultural background and social norms influencing individuals' response to cyberattack emails (Alhasan, 2023; Klein et al., 2019; Parsons et al., 2010). The current study extends the previous work on cultural background and cybersecurity to explore which forms of communication in relation to memorable messages have a role in adopting secure behavior among Saudi students abroad. More importantly, the current study extends the work to find if cultural background is present in expressing memorable messages concerning secure information data. Therefore, the following research question will guide identifying patterns and themes in the memorable messages that encourage Saudi students abroad to adopt secure behavior in less familiar interactions.

RQ3: In what ways did a key message (e.g., cultural, religious, content, sources) influence Saudi students to adopt protective behavior against fraud in unfamiliar environments?

In the context of anti-fraud-related messages, the current study suggests that identifying participants' specific memorable messages is crucial for determining which communication materials effectively influence protective behaviors. This assertion is based in applied communication studies, where researchers utilize grounded theory and practical approaches to address real-world issues to tackle issues (Barge & Craig, 2009; Berger, 199; Keyton et al., 2009). For example, Nazione et al. (2011) used a grounded approach to identify memorable messages that helped students navigate college life by interviewing 61 undergraduate students who recalled a specific message that helped them navigate college. The findings of Nazione et al. (2001) included categories of messages that were later discussed with college personnel, emphasizing the relevance and practical implications of the research findings within the college environment. Therefore, the current exploration study examines which communication forms, particularly MMs carried by Saudi students abroad, influenced their secure behaviors, which further contributes to the growing body of knowledge on preventing social engineering attacks and developing effective risk communication strategies while addressing the unique challenges often faced by Saudi students abroad. Thus, this inquiry was structured around the following research question. The following research question guided the study to a wide range of strategies for crafted messages to effectively alter attitudes toward the threat of SEAs, which encourage protective measures among vulnerable populations, including students abroad in foreign countries.

RQ4: In what ways are memorable messages and taking secure behaviors linked among Saudi students abroad?

The memorable messages framework was also used within organizational cultures. Stohl (1986) revealed that employees remembered specific messages that impacted their work experiences and influenced them to be integrated into the work culture. Further, Stohl's research findings outlined the standards for appropriate behavior within a company and helped to assimilate individuals into the work culture. Kaufmann et al. (2021) also explored school students' memorable messages that influenced their motivation and performance during the COVID-19 pandemic. The study revealed that memorable messages received from the students' instructors significantly impacted students. Further, they introduced a practical implication for instructors' future communication practices with students. More importantly, Kaufmann et al. (2021) highlighted the role of emotions such as stress and fear during uncertain times, which particularly enhances the long-lasting impact and influence of the received messages. Therefore, the current study focuses on students abroad who experience uncertainty during the cultural transition, limited knowledge of local and financial systems, and financial vulnerability, all of which are heightened by stress and ambiguity. Furthermore, Barge and Schlueter (2004) also emphasize how communication relates to messages as they found its role in shaping the relationship between newcomers' integration into the organization. Barge and Schlueter (2004) particularly guided their exploration through the memorable messages framework to examine the socialization discourse during organizational entry experiences. They found that it plays a significant role in constructing relationships and fostering motivation and engagement during the *fitting in* process.

Considering the critical role of anti-fraud initiatives in raising individuals' knowledge against SEA threats, several researchers have evaluated such efforts, mainly focusing on the public anti-fraud campaign. Thus, several researchers advocate utilizing methodologies such as

direct response tracking, framing analysis, and rolling sample surveys to appraise the effectiveness of campaign materials and messages (Chugh & Narang, 2023; Coffman, 2002; Hall, 2002). However, as indicated by Chugh and Narang (2023), basic surveys that monitor self-reported behavior often prove inadequate due to behavioral biases, including experience factors, motivation, and personality traits, which prompt individuals to act irrationally. Based on their pilot study, they found that simply raising awareness does not always lead to changes in attitudes. Therefore, they proposed that campaigns should also address the management of individuals' emotional states, "*hot states,*" to positively influence attitudinal change and significantly improve the campaign's effectiveness. Accordingly, Chugh and Narang (2023) have created a framework to evaluate the effectiveness of awareness campaigns better (see Figure 1), illustrating the sequential relationship between three essential steps that assess the efficacy of a campaign in raising awareness against fraud activities, which involves a combination of message components (Appeal) and receiver reactions (Recall and Comprehensibility).

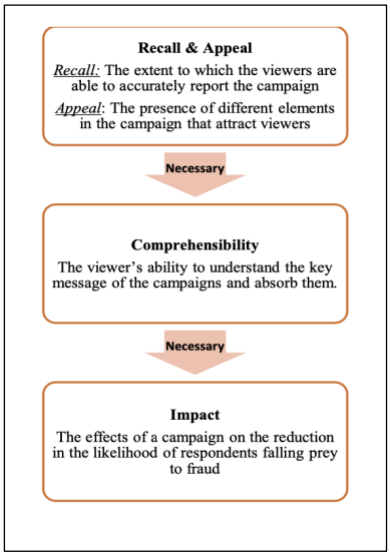


Figure 1: *Framework for Assessing Effectiveness of Awareness Campaigns by Chugh & Narang, (2023).*

The concept of recalling specific messages, introduced by Knapp et al. (1981), has served as a foundation for several applied research. However, we found limited exploration of memorable communication events and messages in shaping individuals' secure behavior. The current study explores the messages lead to an increase in students' recognition and concerns of scam threats, which have been found to include instructional messages and media messages addressing fraudulent activities, to determine their forms in influencing individual secure behavior (Razaq et al., 2021; Van Bavel et al., 2019).

Several studies have explored which communication strategies promoted behavior change, highlighting the role of interpersonal conversations to message memorability in influencing decision-making. For instance, Hinyard and Kreuter (2007) found that conversations were powerful tools for influencing health behavior by making information relatable and engaging. Similarly, Ogata Jones et al. (2006) demonstrated that combining exposure to mass media messages with interpersonal communication effectively promoted women's breast cancer screening practices. Expanding on this, Davis et al. (2016) identified the memorable messages framework as a crucial framework for understanding which message has the most significant impact, they have emphasized that personal relevance and message vividness enhanced message retention and memorability. In the context of secure practices, Albrechtsen and Hovden (2010) found that interactive approaches, such as employee dialogue and small workshop programs, were more effective in prompting security awareness and behavior than passive approaches like formal presentations or security emails. Collectively, these studies highlighted the importance of engagement and relatability in enhancing communication memorability and driving behavioral change.

Synthesizing prior studies in which communicated messages enhanced individual behavior, particularly during the integration into a new environment, where foreign students faced less familiarity with and misunderstanding of culture and social interaction practices (Andrade, 2006; Baklashova & Kazakov, 2016). Considering that the effectiveness of secure messages in influencing behavior—such as media messages or storytelling—may be heightened when tailored to individuals and made personally relevant, it is crucial to avoid overwhelming audiences with generalized advice, as not everyone requires the same level or type of guidance (Cialdini, 2009; Hinyard & Kreuter, 2007; Redmiles et al., 2016). This investigation into fraud avoidance behavior and communication forms influencing these decisions builds on previous research.

CHAPTER 3: METHOD

Overview

In the current chapter, the researcher describes an overview of the study methodology, data collection, survey development, participant selection, study design, and data analysis phases (i.e., data coding phases, categories phases, and reporting themes extracted from the data coded). This is followed by the researcher's validation strategies for data accuracy. The purpose of the qualitative exploratory case study inquiry was to develop an understanding of whether communication forms in relation to memorable messages (Knapp et al., 1981) that Saudi students abroad carry with them influenced secure behavior in less familiar environments, which served as an initial link between memorable communication messages/events and secure behavior to avoid social engineering attacks. The lens of exploring fraud avoidance behavior was best seen to adopt the inductive exploratory approach, in which the researcher focuses on constructing an understanding of the issues through the participants' lived experiences and interactions (Creswell & Creswell, 2017; Jebb et al., 2017; Swedberg, 2020).

In the current inquiry, the qualitative method is emphasized by the necessity of gathering unstructured data to explore the relationship between participants' memorable communication events and the adoption of secure practices against SEAs in less familiar interactions. Consequently, clarifying the gaps in understanding what and how memorable messages impact protective behavior among a specific group such as Saudi students abroad opens up valuable avenues for future studies in the area of communication studies and behavior change. For that purpose, analysis involved inductive qualitative content analysis where the researcher identifies themes and patterns that reveal how Saudi students studying in Western countries fraud-related experiences with fraud avoidance and protection in less familiar environments. The iterative

nature of inductive qualitative content analysis (i.e., seeking to explore a phenomenon and comparing data throughout the analysis process) allowed the researcher to determine the new insights emerge (Elo & Kyngäs, 2008), as well as observe the participants' unique stories and experiences that they shared in response to fraudulent threats. What is more, the inductive qualitative content analysis technique facilitated a deeper exploration of the factors influencing the behavior of Saudi students abroad in navigating secure technology-human-based interaction, considering cultural differences, and adopting secure actions to protect themselves against potential scams.

Participant Selection

For this study, a purposive sampling method was utilized, which is a non-probability technique that selects information-rich cases based on specific characteristics relevant to the study, providing valuable insights into the central issues of the inquiry (Gentles et al., 2015; Patton, 1987). An online survey was available from October 20th, 2024, to December 15th, 2024. A total of 225 Saudi students studying in the United States, United Kingdom, and Australia completed the survey. The total sample size included in the analysis process consists of 72 out of 225 participants, all of whom were eligible based on the study objectives and who met the following inclusion criteria:

- Saudi Students located in one of the Western universities, including the U.S., the UK and Australia
- Students who are 18 years of age or older
- Students who have taken at least one secure action from a predefined checklist to protect themselves against SEAs
- Students who have answered at least one of the open-ended questions

Participants consisted of 39 males and 33 females. All participants were Saudi students studying abroad in Western countries, with 14 in the United Kingdom, 10 in Australia, and 48 in the United States. Table 1 presents the basic demographic information of the study population, including their age, gender, education level, Western country enrolment, and the Saudi Arabian region from which they are.

Table 1

The Demographic Characteristics of Participants

Variables	*n*	(%)
Age		
18-24	5	6.94
25-34	34	47.22
35-44	29	40.28
45-54	3	4.17
55-64	1	1.30
Gender		
Male	39	54.16
Female	33	45.83
Education		
High School	3	4.17
Bachelor	16	22.22
Graduate	51	70.83
Not Mentioned	2	2.78
Country enrolment		
The United States	48	66.67
The United Kingdom	14	19.44
Australia	10	13.89
***Saudi Arabian Regions**		
Central Region Western	21	29.16
Region Eastern Region	22	30.55
Northern Region	13	18.05
Southwestern Region	4	5.55
Not Mentioned	11	15.27
	1	1.38
	N= 72	

*The Central Regions are Riyadh and Qassim, the Western Regions are Makkah and Al-Medina, the Eastern Regions are Eastern Province, the Northern Regions are Hail, the northern borders regions are Al-Jouf and Tabouk, and the Southwestern Regions are Aseer, Al-Baha, Jazan, and Najran

Additionally, Table 2 presents descriptive statistics that provide an overview of the study sample based on participants' experiences with social engineering attacks. These statistics reflect four groups of participants: (a) victims who have suffered harmful SEA attacks, including financial loss; (b) non-victims who were exposed to fraud-related stories from close others; (c) participants who engaged in suspicious interactions with scammers but did not incur any losses; and (d) participants who did not share their stories behind their secure behavior. The last group of participants was excluded from the data coding since they did not provide any narrative to the open-ended questions.

Table 2

Sample Characteristics

Participant Group	*N*	*%*
Victims of SEAs[1]	22	9.77
Not Victims of SEAs, But[2]		
Indirectly Exposed Suspicious Interaction	50	22.22
No Shared Reason[3]	153	68.00
	N = 225	

1=Social engineers' attacks Victims 2= Exposed to close-others fraud-related stories and/or engaged in suspicious interaction with scammers 3=Participants group who did not share their story of why they take secure actions against SEAs.

Given that the current study focusing on Saudi students currently studying in Western countries under the Saudi Arabia educational mission. It is worth mentioning that the Saudi Education Mission, established in 1927, aims to facilitate Saudi students in pursuing their higher education in various countries worldwide (Abdullah, 2022; Al-Hamzah, 2022). During the study time, according to the Ministry of Education in Saudi Arabia, data shows that nearly 37,000 Saudi students are pursuing their education in Western countries, with approximately 17.000 in the U.S.,

16,000 in the UK, and 4,000 in Australia (Ministry of Education Statistics, n.d.; see Appendix B). Moreover, several reasons exist for choosing Saudi students abroad as a population from which to sample rather than local U.S.-based students. First, in addition to the abroad students' susceptibility to being victims of social engineering attacks in less familiar interactions, which has been observed among local college students as well (Bleiman & Rege, 2020; Rege, 2019), this selection was employed by the researcher to understand whether forms of communication were memorable or other factors including culture, social, and personal have guided students abroad to protective behavior against security risks. Furthermore, the selection was also influenced by the shared context of the experience of studying in one of the Western countries between the researcher and the selected sample, in which both have experienced new cultural norms and less familiar interaction norms, as well as the need to manage the security risks outside of Saudi Arabia.

Second, the selection of Saudi Students abroad as a case study allowed the exploration of whether memorable communication forms influenced the adoption of more secure behavior, particularly given the challenges of experiencing cultural and language differences and less familiarity with local system interactions. Given that the study population consists of Saudi students abroad, these individuals are expected to practice a unique culture of personal interaction characterized by strong family ties, Islamic values, and social expectations (Alsanea, 2023; Alyahya & Weir, 2021). As a result, the findings of the current inquiry may resonate with the context of Saudi Arabia and other collectivistic cultures.

Design And Procedures

Memorable messages and their communication sitting in SEAs represent a relatively new area of research within communication studies; however, determining the features of memorable messages might offer contributions to enhance the risk communication strategies to combat such

threats. Thus, the current study sought to address these gaps in the communication literature and identify the features of increasing communication memorability and secure behavior adoption among Saudi students abroad. Therefore, the selected research design of this exploratory study was inductive qualitative content analysis, in which the researcher explored the fraud-related lived experiences among the Saudi students studying abroad during their less familiar interactions. Following an inductive approach was especially meaningful in exploratory qualitative research to answer the research questions. To do that, rather than starting with pre-established categories, the inductive process allowed categories and themes to emerge organically from the participants' inputs (Azungah, 2018; Thomas, 2006). The process of coding samples and development steps is included in Appendices C, D and E , which are based on and generated from the participants' fraud-related stories and messages. From the current design perspective, the researcher explores a social phenomenon through the lens of individuals' experiences, actively reflecting on their complex cultural context and social interaction (Geer, 1988; Popping, 2015). To achieve this, the research design utilized an open-ended online questionnaire that allowed participants to share their stories and messages that motivated and influenced their behavioral change in their own words. Generally, qualitative research has been explained as the process of exploring and understanding social reality and phenomena within a society (Creswell & Poth, 2016; Creswell & Creswell, 2017).

Considering the purpose of the current study to develop answers to the 'what initially' and 'how' questions regarding secure behavioral adoption to avoid social engineering attacks, other qualitative research designs were less suitable. The nature of the exploratory study has been highlighted by Ghauri et al. (2020), who stated that the primary aspect of the exploratory study is to gain insights that can contribute to a deeper understanding and inform future studies. In other words, the process of collecting data to identify patterns among the selected cases (i.e., Saudi

students abroad) would initially produce sufficient information on the nature of the social issue under study and its relationship with other contexts or factors (i.e., communication forms, messages, social, cultures factors; Denzin & Lincoln, 2011; Stake, 2008). Further, the use of inductive, exploratory approach is commonly used where the researcher attempts to identify a social issue that has not been deeply investigated or in cases where there are still gaps in the related materials that need to be revealed to address the problem (Ghauri et al., 2020; Swedberg, 2020).

However, several studies have revealed a critical challenge associated with the exploratory study nature, including the uncertainty of whether a valuable finding will be found or whether meaningful insights from the data collected will be extracted (Stebbins, 2001; Swedberg, 2020). Nevertheless, the nature of an exploratory study is valuable when the researcher can determine factors and social phenomenon in answer to research questions (Mathkur, 2019; Saunders et al., 2018). Overall, an exploration case study design was best with the open-ended study since the intention was mainly to generate initial concepts for further study on whether forms of communication, particularly memorable messages, as a determining factor in decision-making for Saudi students aboard to be more secure to protect their financial and informative data, rather than to examine the issue of trauma of fraud victimization.

In the current study, the researcher collected unstructured data through an open-ended online questionnaire using OU Qualtrics software (see Appendix A), which is a valuable tool encouraging detailed and personalized responses from the study participants (Looker et al., 1989). The study recruited participants through emails sent by the Saudi Arabian Cultural Mission to the USA. The survey was completed online, and it took participants an estimated 7 to 12 minutes to answer the questions. The rationale behind the section of an open-ended survey as a method of collecting data was to allow the participants to respond in their own words, offering valuable insights that closed-

ended surveys might overlook (Patton, 2014).Further, in this research, we critically aimed to use open-ended questions to gather diverse and nuanced stories from participants to identify whether communication forms influenced students to take secure actions against fraud expressed in their distinctive experiences. Open-ended survey questions are often used as a qualitative tool to capture detailed personal experiences and gain a deep understanding of behaviors and attitudes (Creswell & Poth, 2016). It also might offer valuable insights into individuals' lived experiences regarding the social phenomena under study (Creswell, 1994; Guba & Lincoln, 1994; Patton, 1987). However, given that in qualitative studies, researchers seek to achieve rigor in the data to draw meaningful conclusions, several studies expressed their concern about using open-ended survey questions. One is that some individuals may have challenges in clearly articulating their experiences and views (i.e., communication skills, which may lead to incomplete answers due to difficulty expressing themselves rather than lacking valuable information; Geer, 1988; LaDonna et al., 2018). Further, Geer (1988) was concerned about the challenges in analyzing participants' answers, which depend on the human coder's ability to use rigorous qualitative procedures and convey an accurate interpretation of the data. Given that, the researcher is mindful of the challenges associated with using free-response survey questions, including potential misinterpretation of the participant's answers, time-consuming systematic analysis of open-ended data, and variability in the depth of participants' responses. To address these challenges, several techniques, including Tracy's big tent criteria and Creswell (2007) validation strategies were employed to increase the validate of qualitative data. These techniques are discussed in the following validation strategies sections.

For collecting meaningful and specific qualitative data the survey includes seven questions alongside five demographic questions, using a combination of two close-ended questions and six

open-ended questions (see Appendix A). One question consisted of multiple choice pre-validated secure actions (Ion et al., 2015), in which students had to select at least one secure action they practiced protecting themselves from SEAs as one of the sampling criteria. Another close-ended question was a Likert scale statement that consisted of options ranging from "Very Concerned" to Not Concerned at All," in which participants were asked to rate their level of concern about social engineering attacks' risk. The other six questions serve to gather narratives and unstructured data using free-response questions. These questions were later restructured and polished through feedback from the dissertation committee members to ensure alignment with the study's goals, enhance relevance, and address any sensitivity concerns. The refinement of the survey questions process is particularly common in dissertation studies, often supporting the improvement of the quality of data collected that would reflect on the validation of the study outcome as well. In addition, the process is also crucial during the design of free-response questions, which could encourage participants to provide more meaningful and relevant narratives (Popping, 2015; Revilla et al., 2019). Because the purposive sampling consisted of Saudi students studying in Western countries, including the U.S., UK, and Australia, who represented various levels of education, including the English acquisition stage, the survey questions were available in both languages.

Survey questions were initially written in English, but were later translated into Arabic by the researcher herself due to her Arabic mother's language. Furthermore, participants were informed that their answers could be provided in their preferred language, either English or Arabic, to ensure smooth expression of their memorable communications associated with their decision to change behavior against SEAs while answering the survey questions. The translation and the research overview's cultural appropriateness to the Saudi Arabia culture were accomplished through the assistance of a third party who had expertise in conducting a study with the same

population (i.e., Saudi students studying in Western countries), specifically in the United States, as well as his fluency in both languages as a way of avoiding any error or issues. The third-party person was introduced to and confirmed by the IRB at the University of Oklahoma.

The use of the survey questions was based on considering previous studies to ensure the quality and consistency of the collected data, as well as to contribute to and compare the findings with existing literature on understanding interactions and messages influencing behavior change specifically regarding secure behavior adoption. Thus, the participants answered the survey questions in the following sections:

Mandatory Prescreening for Eligibility

Every participant was required to answer a question about eligibility, which ensured that the collected data represents the purposive sample of students who have taken secure measures to protect themselves from fraud attacks. This yields reliable, meaningful data aligned with the study objectives. Given that the current study targeted students with varying educational achievements and technological skills. Accordingly, we incorporated the security recommendations from Ion et al. (2015) to enhance our prescreening security procedures, which experts widely endorse. These recommendations include up to 20 security tips, such as software updates, two-factor authentication, antivirus software, and robust password protocols. Some of these were rephrased with non-experts for clarity and relevance before inclusion in the current study. Articulating these recommendations in actionable terms enhanced participants' understanding of study objectives, comprehension of social engineering threats, and recall of related information.

Concern About Fraud Attacks

The respondents rated their concern about social engineering attacks on a 5-point Likert scale from 'Very Concerned' to 'Not Concerned at All.' Concern is viewed as a feeling of unease about

an issue, essential for individuals (Alston, 1969; Winnicott, 1963). It signifies a blend of mind and feeling, fostering responsibility for desired outcomes. In examining participants' feelings about SEAs abroad, Parr et al. (1992) found that international students in the U.S. expressed positive emotions—determination, gratitude, and confidence—but also worries concerning finances, cultural differences, and academic support. Several studies highlight the link between concern and behavior change. Loewenstein et al. (2001) demonstrated that individual decisions stem from risk-as-feelings, emphasizing the role of emotional reactions, like concern or fear, and cognitive assessments in decision-making. Perceived risk significantly shapes behavior, influencing protective measures (Witte, 1992), where increased concern suggests a higher likelihood of taking protective actions (Rogers, 1983). Exploring participants' concern levels offers insights into data. It can enhance understanding of respondents' narratives in free-text responses, improving data analysis (Creswell et al., 2011; Varpio et al., 2022). Combining closed-ended with open-ended questions can clarify how concern levels manifest, enriching the interpretation of responses in context to secure behavior.

Incidents Shaping Concern

In this context, asking participants to describe stories that raised their concerns about the social engineers' attacks would likely evoke the memorable moments that shaped their secure decisions. These narratives might reflect participants' unique experiences of exposure to various forms of communication, offering insight into how such exposure shapes their level of concern about SEAs. That is the combination of first rating the level of concern (i.e., emotion, and then describing the "why" reasoning); responders were encouraged to provide real-life experiences, which can reveal specific interactions, moments, and messages that effectively promoted the adoption of secure behavior, particularly outside of Saudi Arabia.

Recalling Impactful Incidents

The previous question addressed participants' concerns about fraud, while the current question investigates memorable fraud-related stories or incidents. This, along with questions Q3, Q4, and Q5, examines if a specific form of communication stood out. Prior studies have shown that memorable messages can influence behavior, particularly in health contexts (Anderson et al., 2020; Cooke-Jackson & Rubinsky, 2023; Kuang et al., 2023; Smith et al., 2009). This study aims to determine if certain messages were memorable, prompting participants to adopt secure behaviors. It also identifies whether certain communication sources resonated with participants in promoting secure behavior. For instance, frequently mentioned sources may indicate more memorable preventative material. Cognitive studies reveal difficulties people face when answering questions, such as recalling events, misinterpretations of timing, question comprehension issues, and other mental processes (Bradburn et al., 1987; Tourangeau et al., 2000; Willis, 2004). To help respondents recall relevant information and answer effectively, examples were included to illustrate potential sources impacting their secure action adoption, such as news reports, personal experiences, social media posts, and peer experiences. Improving accuracy and encouraging detailed responses during qualitative data collection is crucial; these examples may prompt respondents to consider contexts they might overlook as influential, like peer influence or social media.

Remembering Fraud Avoidance

At this point in the survey, the goal was to encourage respondents to elaborate on their experiences with avoiding fraud, capturing rich information that might have been missed earlier. As these free responses were optional, participants were only asked to provide valuable insights into behavioral change in response to social engineering attacks, rather than providing unrelated

data. These personal experiences highlighted patterns and added depth to our data analysis. In qualitative research, such detailed responses enhance interpretation and allow for nuanced understanding of behavior change and complex issues (Creswell & Poth, 2016; Lewis, 2015), particularly in adopting secure actions influenced by individual context (Alotaibi et al., 2016; Van Bavel et al., 2019).

Remembering Fraud Experiences

In this context, the survey questions asked respondents to recall a broader range of fraud-related instances, including experiences of others, such as relatives and friends. We recognized that not all respondents may have faced fraud attempts personally, but their peers could have. Interpersonal communication influences behaviors and attitudes towards risk (Andrews & Boyle, 2008; Waldron et al., 2023). This highlighted the role of others' fraud experiences in motivating Saudi students to adopt secure behaviors in unfamiliar interactions. Learning and attitude develop within social situations, influenced by interaction and imitation of more knowledgeable individuals (Bandura, 1986; Vygotsky, 1978). Recently, communication technology has enhanced social learning, showing how people learn together and create a collective mind, as online communities facilitate idea-sharing and learning from one another (Bingham & Conner, 2010).

Recalling Protective Messages

As the current study aimed to explore forms of communication events, a key focus was identifying whether the concept of memorable messages introduced by Knapp and Reardon (1981) has influenced participants to take secure actions to protect themselves from social engineering attacks. This concept refers to statements that individuals perceive as impactful, typically containing influential guidance, warnings, or advice affecting decision-making. Memorable messages have been shown to influence individual behaviors, especially in health-related contexts

where they warn against risky practices and diseases (Anderson et al., 2020; Cooke-Jackson & Rubinsky, 2021, 2023). Furthermore, messages generally have a significant impact, particularly when constructed emotionally positively, socially contextual, and relevant to people (Dunleavy & Yang, 2015; Kaufmann et al., 2021; Lucas & Buzzanell, 2012). In light of this, the study's primary focus was to extend the work into social engineers' avoidance and examine whether memorable messages influenced participants to adopt secure behavior during their journey in less familiar cultures and interactions in Western countries.

Demographic Information

Five demographic questions were given to respondents in the last part of the survey. These multi-choice questions included the respondents' gender, age, educational level, the Saudi region, and the current country they are studying in "optional." In this context, collecting demographic information serve to understand how different factors influence respondents' secure behaviors and memorable communication events in new cultures and interactions. In a qualitative study, demographic information facilitates data interpretation within its relevant context; this provides deeper insights into the generated patterns, addresses biases, as well as contextualizes the findings. The final part of the survey involves thanking the participants for their contributions and asking for their contact information if they are interested in discussing their in-depth responses.

Ethical Considerations and Recruitment

The current study received approval from the Institutional Review Board for the Protection of Human Subjects. The University of Oklahoma under protocol number #17813. All participants were informed about the study's purpose, confidentiality measure and their right to withdraw at any time. All participants were recruited through an email sent by the Saudi Education Research Center to Saudi students through an online open-ended survey; this center supports Saudi Arabian

graduate students in distributing surveys to the target population. The email contained brief information along with the survey link, which included details about the researcher, the study's purposes, and the study participants' targets. Informed consent was obtained electronically, as all participants had to accept (i.e., Yes, I agree to participate to be part of the study before displaying the survey questions). Additionally, participants had to confirm their national origin and age (i.e., Are you a Saudi student studying in the United States, United Kingdom, or Australia who is 18 or older?). Participants who clicked “yes” were then able to view the rest of the survey questions. Further questions were optional, and participants could pass the question if they had no related information to share. This approach reduced the sharing of superficial information to complete the survey; it also could enhance the data's quality and relatability, offering in-depth conclusions. Participants were given sufficient space for their responses. They were encouraged to take their time recalling information related to financial and informative attack incidents, whether these were messages, stories, or personal experiences that played a role in influencing their concern about fraud, fostering them to make secure behavior.

Data Analysis

In qualitative research, it is crucial that data analysis comply with systematic principles (Pratt, 2009). Given the complexity of analyzing unstructured data, qualitative researchers are encouraged to use computer-assisted qualitative data analysis software that allows them to organize and manage the data (Bringer et al., 2006; Nobles, 2021). Generally, in qualitative data analysis, the researcher engages in steps such as, organizing the data, familiarizing with the data, coding and categorizing the data relevant to the study objectives into themes, creating the interpretation of the themes, and reporting and visualizing the themes (Creswell & Creswell, 2017). Given the exploration nature of the current study, the data analysis process drew on

inductive qualitative content analysis techniques (Thomas, 2006). This approach was designed to categorize repeated keywords and answers into structural and meaningful themes about participants' experiences in which a theory or concepts develop (Strauss & Corbin, 1990; Saunders et al., 2018). The inductive qualitative content analysis process involved a four-step analysis protocol: After reading and rereading the data, the researcher conducted four analytic steps: open coding, focused coding, subthemes development, analysis and interpretation. The following subsection provides a detailed description of the data analysis phases based of the inductive qualitative content analysis (Hsieh & Shannon, 2005; Thomas, 2006).

Familiarization

Transcripts were uploaded from the OU Qualtrics software to Microsoft Excel, and then the researcher read and reread the participants' responses to gain an overall understanding of the data. This process helped the researcher become familiar with the data and effectively grasp the nuances and potential patterns within it before the coding process (Creswell & Creswell, 2017).

Open Coding

After the researcher thoroughly read the entire answers given by 72 participants, the researcher could highlight stories and incidents relevant to the research questions. The first step of analysis involved the initial coding process, which involved grouping participants' responses and assigning them to appropriate summative codes or labels (Popping, 2015). To ensure consistency in data analysis, each code highlights the significance and meaning of the corresponding data segments (Corbin & Strauss, 2015; Saldaña, 2021). Furthermore, several studies have highlighted the importance of open coding phases for researchers to evaluate the respondent's experiences progressively in relation to the matters being studied (Nobles, 2021; Thornberg & Charmaz, 2014). In the open coding phase, the researcher created a Microsoft Word document to label and

categorize the data relevant to the study questions into several categories (Appendix C). Each open-ended question was coded in a separate coding table that consisted of several categories representing the participants' answers. This table was used to categorize responses from each open-ended survey question. While most data aligned with similar labels across questions, unique labels emerged for responses to questions 6 and 7, as these two questions asked participants to specifically share memorable messages encouraging the adoption of secure actions, while other survey questions were mainly asked to share fraud-related incidents or stories (Appendix E). The open code tables served as an initial codebook containing inductively-generated categories that represent recurring and similar stories and messages in the participants' responses. In this phase, to address the validity and reliability of the generated categories, the researcher conducted multiple rounds of revision until theoretical saturation was achieved for the entire data set. In this process, the repetitive nature of the participants' responses was considered, and no emergent categories were identified from the data (Guest et al., 2006; Patton, 2014).

Focused Coding

In the second step, a large set of initial categories emerged from the data during the initial coding phase. Therefore, to refine the explanatory power of categories, the researcher sought to narrow down the number of categories and synthesize them to maintain coherence and relevance across the categories (Charmaz, 2006; Corbin & Strauss, 2015). Thus, the initial categories were reviewed and synthesized to create categories aligned with the research objectives. For example, the initial coding identified 21 categories, which were later refined and incorporated only 17 categories (see Appendix D). For example, in the focused coding stage, categories related to participants' experiences with scammers impersonating official entities and those exploiting trust in such entities were combined into a single category-named suspicious interaction. The validity

and reliability in this phase were also achieved when the researcher continued finalizing the codes until they were all accounted for by an appropriate category, illustrating the potential connections between the generated categories and the study objectives.

Subthemes Development

The purpose of the current phase was to create meaningful and consistent subthemes; these subthemes would allow the researcher to comprehend the connections in relation to categories in terms of context and conditions (Charmaz, 2006). In this stage, the researcher theorized the interrelationship among the categories related to the study questions. For example, related categories were grouped into subthemes that aligned with the forms of communication reflected in the responses. Categories, such as family and friends' negative experiences and peers' negative experiences, were combined under the subtheme of interpersonal communication (close-others), which included participants' responses to stories they heard or shared within and beyond their social environment. Meanwhile, categories like personal negative experiences with fraud and suspicious interaction were classified under the subtheme of interpersonal communication (own), representing participants' encounters with scammers through communication channels such as text messages or scam calls. This far and given that the final coding categories were not mutually exclusive, as participants' responses often reflected overlapping subthemes. As result, traditional reliability measures such as inter-coder agreement were not applicable. Instead, a peer review was conducted across two sections in which a second scholar cross-checked approximately 10% of the coded data and provided feedback on the categories and subthemes' consistency and interpretation, resulting in renaming some of the terms used to align the research questions better.

Analysis and Interpretation

The purpose of this phase is that the core theme integrates all other subthemes developed during the prior phase, allowing the researcher to theoretically explain the central phenomenon under study (Corbin & Strauss, 2015). In this final stage, the related subthemes were grouped into predominant themes that captured the broader patterns in the participants' responses. For example, the subtheme of intrapersonal and interpersonal communication were incorporated into a broader theme referred to as interactive communication in fraud awareness. This theme highlights the role of interactivity in enhancing the memorability of fraud-related incidents, influencing the concern about fraud, and making it more likely that participants adopt secure behavior (See Table 6). At this point, the researcher identified the primary relationship between adopting secure behavior and memorable messages to address the gaps further and create a coherent, meaningful concept. Furthermore, the process of creating a concept explaining which memorable communication strategy impacts concern about fraud and fostering fraud avoidance behavior among participants has devolved. Lastly, the current stage completes the data analysis phases by ensuring that the data and themes cohesively explain the theoretical framework of secure behavior against social engineer attacks.

Validation Strategies

This section outlines the strategies used to ensure the validation of the qualitative data as applied in this study. In this research, following an inductive qualitative content analysis approach, the researcher assesses the rigor and accuracy of the findings throughout the study process by using several qualitative validation strategies drawn from Creswell's (2007) outlined validation methods. First, in line with Tracy's (2010) criteria for high-quality qualitative research, the current study addressed a "*worthy topic*" by explaining the challenges Saudi students studying abroad face in navigating less familiar interactions and avoiding prevalent

fraud attacks. Generally, international students frequently face several challenges associated with cultural differences and communication difficulties, this also including the widespread malicious fraud attempts targeting their information, such as fake job offers, fraudulent emails from fake government requests, and phone calls falsely accusing illegal activity under their name (Akanwa, 2015; Gonzalez, 2024; Marginson, 2012; Simulated Phishing Update, 2024). By exploring the memorable communication messages/events that influenced the adoption of secure behaviors among Saudi students abroad, this study provides a "*significant contribution*" to identifying effective risk communication strategies. Additionally, the current research ensures archiving *"rich rigor"* by exploring and analyzing lived experiences; this provides an in-depth analysis of the complexity of the link between memorable communication events and secure behavior against social engineering attacks.

One technique to establish validation was to enhance the credibility of the study findings by introducing and explaining the negative cases. In qualitative research, to enhance credibility, increase the rigor of the findings, and strengthen the accuracy of the research results the researcher refines their interpretation and considers the various perspectives present in the data, including those that contradict the emerging patterns of the study (Creswell & Miller, 2000; Hanson, 2017). Furthermore, in qualitative studies, while the search for confirming evidence to support preliminary themes or categories is common, searching for and presenting disconfirming evidence found in the data enhances the credibility of the findings and accounts for the multiple and complex nature of social reality (Creswell & Miller, 2000)**.** To do so, the researcher presented the participants' experiences that contradict the patterns of the dominant experiences found within the data. The study considers participants who reported being unconcerned about fraud risk as negative or deviant cases that challenge the dominant patterns of concern expressed

by most participants (Creswell & Miller, 2000; Hanson, 2017). Unlike other participants, they remained unconcerned even though several (n=7) had either experienced harm from scam attacks or engaged in suspicious interactions with scammers. For example, one participant mentioned, "نعم وردني اكثر من اتصال والهدف منه السرقة وهم يستغلون بشكل كبير حاجز اللغة مع الطلاب المبتعثين." (Yes, I have received more than one call with the aim of stealing, and they greatly exploit the language barrier with students abroad.) Another participant added, " تمت سرقة معلومات بطاقتي في السابق وتم سرقة ٨٠٠ دولار " (My card information was previously stolen and $800 was stolen.). Additionally, a validity procedure for researcher reflexivity was utilized to enhance and maintain the credibility and transparency of the study process and findings, ensuring alignment with its objectives. The researcher created two separate sections on the "Research Positionality" and "Assumptions" to reflect on the cultural background and beliefs that may shape the orientation of the study, particularly the data analysis and interpretation (Creswell & Miller, 2000; Merriam & Tisdell, 2009**).** In that, the researcher openly acknowledged her subjective aspect in selecting the Saudi students abroad in Western countries as a purposive sampling in this study rather than other local students, in which Saudi Arabian cultural and social values comprehension was meaningful and might influence the interpretations.

Considering that the researcher has minimized biases in interpreting the participants' responses, some latent language the Saudi Arabian people used to express their experiences required familiarity with the local Saudi dialect for proper understanding and interpretation. For example, one participant mentioned in response to the question about a memorable message that led to adopting secure behavior, said "نصيحتي عدم الشماته بأي شخص تم النصب عليه لأن الدنيا داره" (My advice is not to mocking over anyone who has been scammed because life is cyclical; "Life is fickle"). This response was not easily translated into English, as the phrase "life goes in cycles

“Life is fickle”)” requires further interpretation from the researcher to explain the common belief deeply rooted in Islamic and Arab culture, where mocking others is seen as potentially leading to a similar situation in the future. This response was categorized as a wisdom-based message, a common expression in Arabic culture and Islamic teachings, emphasizing that no one is immune to hardship and encouraging social ethics and humility among people. Generally, researchers in a qualitative study do not reject subjective aspects; however, these must be acknowledged in terms of how they might influence the interpretation (Creswell & Creswell, 2017; Noble & Smith, 2015).

Additionally, in a qualitative study, peer debriefing is a procedure used to ensure the credibility of the research. This allows other researchers to support and/or challenge the researcher's findings, interpretations, and conclusions, as these must be aligned with the data (Creswell 2007; Creswell & Miller, 2000). To do so, a systematic coding process was documented in both the initial coding and the development of final themes; these were reviewed through peer debriefing to enhance analytical rigor and minimize the researcher's subjective influence. During the peer debriefing, the emerging subthemes and themes were discussed, and alternative terms for the subthemes were suggested to align the study objectives better. This also included a discussion of the negative cases found during the analysis, resulting in the elimination of the initial negative cases and the replacement of these cases with other cases in the data.

CHAPTER 4: FINDINGS

The current chapter presents the findings derived from the responses of Saudi students studying abroad in Western countries to the open-ended online survey explicitly designed to address the research questions. As previously discussed, recalling specific incidents can be challenging for some individuals, and others may struggle to articulate their thoughts narratively. Therefore, to maintain relevance and focus, participants who did not meet the eligibility criteria and did not answer any of the six open-ended questions, totaling 153 out of 225, were excluded from the analysis. This limitation of inability to remember was identified as one of the challenges in the current study. Therefore, the study findings are based on 72 participants who answered open-ended questions, sharing 404 stories and incidents related to SEAs. These were systematically analyzed to develop categories and subthemes identifying forms of communication that highlighted participants' concerns and encouraged secure behaviors to avoid fraud attacks. Since not all participants provided narratives in response to each question, the analysis concentrated on the amount of fraud-related content rather than individual participants.

furthermore, many participants were also able to recall and share multiple fraud-related incidents across the free-response questions. For example, a participant mentioned in response to a situation that heightened their concerns about fraud, *"In addition to incidents that happened to people I know, the media always has some people warning us about the new ways that attackers follow to deceive people*." Another participant added, *"Peer experiences and media."* These two examples showed that some participants were influenced by multiple communication sources, e.g., interpersonal communication with close others and media messages. Therefore, each source was coded separately into different codes and categories. Through an iterative coding process, 17 categories were developed that reflect the factors influencing participants' concerns and adopting

protective behaviors against SEAs (see Table 3). These categories provided a comprehensive framework for understanding through which participants' stories and messages were associated with communication forms. The data revealed categories reflecting peers' negative experiences with fraud, personal encounters, fraud abroad, suspicious interactions, advanced technology exploitation, vigilance, academic instruction, participants who are not concerned at all, avoidance strategies, cultural wisdom, authority warnings, media messages, and social media posts. Some responses indicated that participants did not recall fraud incidents, or their answers were irrelevant. These were categorized into two groups: those who did not remember incidents and those deemed not applicable, both of which were excluded from the analysis as they lacked relevant insights for the research questions. The categories were organized into six meaningful subthemes representing how participants learned about fraud risk and were encouraged to adopt secure behaviors against such risk. Table 3 provides an overview of the categories, subthemes, and quantity of supporting evidence derived from the data. The subsequent subsection discusses these subthemes and broader themes in detail, addressing each research question.

Table 3

Subthemes and Categories of Participants' Responses Regarding Fraud-related Stories

Subthemes	Categories	Number of references from the data	Description
Interpersonal Communication (close others)	Others' Negative stories with Fraud	68	This includes participants' responses about fraud-related stories from their social circle.
Interpersonal Communication (own)	Personal Negative Experiences with Fraud Personal Negative Experiences with Fraud Abroad Suspicious Interaction	59	This includes participants' responses about fraud-related stories or interactions with scammers through a medium or online networks (e.g., email, text, calls, or social media)

Intrapersonal Communication	Vigilance Against Fraud Avoidance Strategies Culturally Inspired Wisdom Exploiting Advanced Technology	22 60 20 18	This includes participants' responses reflecting their internal anti-fraud awareness, including emotional aspects and behavioral intentions to protect themselves against potential threats.
Institutional Communication	Authority Warnings Academic Instruction Media Messages Social Media Posts	15 4 9 9	This includes participants' responses about messages received from media, organizations, or public campaigns.
Underestimate Fraud Threats	Self-Confidence Trust in Institutional Protection	5 1	This includes responses from participants who are not concerned at all about attacks from social engineers.
Unrecalled or Unrelated to secure behavior or MMs	Do not Remember/Encountered Not Applicable	47 5	This includes participants' responses who either could not remember or whose answers did not fit into a category.
		N = 404	

Note. The total number of responses was 330. The analyses were based on 404 entries, as some participants provided multiple answers within a single response.

RQ1: *What behavioral change did Saudi Arabian students abroad take to protect themselves from social engineers' attacks?*

The research question was addressed by analyzing participants' answers to questions one and 1a from the open-ended survey (see Appendix A). Notably, most eligible respondents indicated they had implemented at least three secure action options (*n*=40). Additionally, a significant number of participants (*n*=25) reported following six or more of the listed actions to protect their financial and personal information from SEAs, (*n*=6) participants adopted one or more of these secure actions, while only one stated that they had implemented all the listed actions. Thus, this highlights that adhering to multiple secure practices demonstrates participants' recognition of the threats associated with fraud attacks. Moreover, although the

variety of secure actions offered in the survey reflects security procedures widely endorsed by security experts (Ion et al., 2015), few participants (n = 13) shared their strategies for avoiding such attacks, in addition to their choices from the listed secure actions (see Table 4). This indicates that participants have developed a sense of caution about the risks associated with social engineering attacks.

Table 4

Secure Actions Against Social Engineering Attacks: Checklist and Additional Participant Strategies

Themes	Statements	*f*	%
Password Management	Changing passwords more frequently to new ones instead of keeping the same password for a long time Not using the same password for different accounts Using two-factor authentication and verification codes [2, 3, 12] Avoiding easy-to-guess passwords like birthdates or names [9]	43	10.85
Social vigilance and communication	Talking with family members and peers about any fraud-related topic Giving attention to the common fraud tactics Learning to Identify phishing and scam tactics [12] Reporting and ignoring scam messages and calls [9] Following fraud prevention advice from schools [8]	81	20.45
Verification Practices	Hang up and call back using the official number when receiving unexpected calls asking for personal info. Avoid downloading attachments or files until you verify the sources. Not answering calls from suspicious/ unknown numbers [1, 5.] Avoiding suspicious links and verifying URLs (.gov, .edu) [4,6, 8] Hanging up on suspicious calls within 15 seconds [10] Verifying unexpected requests for personal information [8]	90	22.72
Proactive practices	Checking your bank accounts often to spot any strange activity. Keeping your phone and computer updated with the latest security fixes Putting money in different accounts as a precaution against fraud[7] Contacting IT/security teams to verify suspicious messages[8.] Using separate accounts/cards for online payments[10] Ensuring websites use HTTPS and are official [12.] Not saving payment card information online unless necessary[13]	83	20.95

Privacy Control	Being careful with what you share on social media about yourself Ignoring requests for money on message apps from known sources. Using VPNs on public networks [12] Shredding sensitive documents before disposal [12] Avoiding suspicious advertisements [11]	99	25.00

Note: Numbers assigned to statements (1–13) represent responses provided by participants.

Table 4 combines ten predefined secure actions with additional protective measures from participants, providing a comprehensive view of their behavioral changes in response to SEAs. These actions are organized into five themes that group similar strategies, emphasizing both technical and interpersonal approaches to SEA risk. Table 4 also shows the frequency of secure behaviors chosen by participants, with each theme representing a distinct fraud prevention approach. Based on the frequency selection, *privacy control* was the most frequently reported category, accounting for 25% of the total selections. In the current analysis, *privacy control*, considered a secure measure, strongly emphasizes safeguarding personal information and limiting exposure, including securing devices and online network accounts. *Verification practices* followed closely at 22.72%, highlighting participants' importance in confirming the legitimacy of communication sources, particularly during phone and online transactions. *Proactive practices* (20.95%) and *social vigilance and communication* (20.45%) were nearly equally frequent, indicating both actively overseeing financial account activists and the importance of talking with others about common attacks. Lastly, the analysis reveals that *password management*, while the least selected practice at 10.85%, still represents a critical technical measure for protecting participants' accounts and personal information.

Furthermore, the additional protective measures shared by participants not only offer insight into their heightened recognition of the fraud risk but also suggest that certain forms of

communication may have encouraged behavioral change. Table 5 presents the additional secure behavior participants shared against SEAs in relation to the form of communication that contributed to adopting such behavior.

Table 5

Subthemes and Categories of Participants' Responses to Secure Practices.

Subthemes	Categories	Examples	Number of references from the data
Institutional Communication		I followed all these instructions from my school[8].	
	Academic Instruction	تعلمت كيفية التعرف على أساليب الهندسة الاجتماعية، مثل رسائل البريد الإلكتروني المزيفة *(Phishing)* والمكالمات الهاتفية الاحتيالية[12] (I learned how to recognize social engineering techniques, like phishing emails and fraudulent phone calls.)	3
		Verify the source of any email, text, or phone message before you respond[8].	
Intrapersonal Communication		*تجنب الرد على الارقام الغريبة وتحويلها للبريد الصوتي*[5] (Avoid answering strange numbers and diverting them to voicemail)	
	Vigilance Against Fraud	*عدم الرد على المكالمات الواردة من أرقام مشكوك بها*[1] (Do not answer calls from suspicious numbers.)	22
		Hang up at the first 15 seconds of any phone call that seems suspicious[10]	
		Avoid suspicious advertisements[11]	
		My phone's / laptop sharing settings are set to 'Contacts Only[2].	
		عدم مشاركة المعلومات الشخصية مع الغرباء . تجاهل مكالمات و رسائل الاحتيال و التبليغ عنها[9] (Do not share personal information with strangers. Ignore scam calls and messages and report them.)	
		I never Trusted digital payment google pay Apple Pay etc. I never save my payment card in any account[13].	*n*=25

Note. The total number of answers to secure actions provided was 13. The analyses were based on 25 entries, as some participants provided multiple secure practices within a single response. Numbers assigned to statements (1–13) represent responses provided by participants.

As Table 5 showed, participants' own strategies were categorized as *safe communication practices*, reflecting efforts to protect personal information when interacting with others, either through mediated communication—such as responding to emails or calls—or while navigating

online transactions, including online payments. Next, these *safe communication practices* were organized based on the elements related to the source of learning these strategies and the participants' comprehension of fraud threats. As shown in Table 5, the first category, *academic instruction*, included responses demonstrating that participants had learned secure behaviors through formal education, highlighting how secure recommendations for avoiding scam attacks contribute to rising fraud recognition. For example, one participant said, "*I followed all these instructions from my school*." Another mentioned that *"* تعلمت كيفية التعرف على أساليب الهندسة الاجتماعية. *"* (I learned how to recognize social engineering techniques).

These responses, along with others shown in Table 5, indicate that participants could recall their institution's security guidelines. These institutions utilized straightforward language that felt familiar to the students, helping them to remember and act upon it. Accordingly highlighting the role of message clarity and institutional influence on behavior change. In the current study, *academic instruction* messages were relayed through mass communication because the information was shared with a segment of the public (i.e., college students) via internet-based courses and emails. Institutional entities, including universities, have utilized email as a communication tool since the 1990s, offering a fast and convenient method for sending information directly to students (D'Souza, 1992; Duran et al., 2005). However, this tool also has several disadvantages compared to face-to-face communication (Byron, 2008; D'Souza, 1992). Some disadvantages are linked to students' motivation to read emails and connect with the intended audience (Simpson et al. 2024), particularly concerning the urgent need to warn students about scam threats.

The second category, *vigilance against fraud*, included responses from nine participants who shared their strategies for interacting securely with others, particularly in navigating online

transactions. This category reflected participants' narratives highlighting their emotional and behavioral responses to avoid potential threats. One example of a quote stated, "*Hang up at the first 15 seconds of any phone call that seems suspicious.*" and *" تجنب الرد على الارقام الغريبة وتحويلها للبريد الصوتي"* (Avoid answering strange numbers and diverting them to voicemail.) Such a strategy showed the participants feeling suspicious, and the behavioral response to that feeling was to ignore these calls and messages. More participants added, " وضع الأموال في حسابات مختلفة *تحسباً لأي عملية احتيال"* (Distributing money across different accounts as a precaution against any fraud.) and "*I never save my payment card in any account*". Both responses demonstrated that participants were distrusted and suspicious (emotional evaluation) and monitored financial activities to detect any unusual activities (behavioral responses).

The idea of *vigilance against fraud* is that participants have shown their anti-SEAs emotions and behavior responses, which refers to individuals recognizing possible threats, feeling suspicion or distrust, and actively taking steps to safeguard themselves. The v*igilance against fraud* category was later incorporated into the theme of *intrapersonal communication*, which emerged from participants demonstrating their internal concern about fraud risk and vigilance to defend themselves against potential threats (see Table 3). Notably, reported secure measures often emerge from participants' experiences or learned behaviors, influencing their mindset of risks, such as being cautious and avoiding suspicious interactions. However, several participants did not provide explicit incidents in which they developed their vigilance against fraud, which led to creating the theme of *intrapersonal communication* as one of the communication forms that promoted participants' secure practices.

Following RQ1a: *Saudi students' abroad level of concern about fraud attacks.*

Data relevant to RQ1a were drawn from participants' answers to question two on the survey, i.e., report level of concern, and question 2a, in which students were asked to describe

incidents that contributed to their current concern about SEAs (see Appendix A). As part of this study, participants' concerns about potential threats to their confidential information are significant and crucial factors in motivating them to adopt safe practices against scammers abroad, as previously discussed (Alston, 1969; Winnicott, 1963). In the current analysis, it was found that although participants stated their SEA recognition by adopting multiple safe actions against fraud as described in the first part of the RQ1, many participants (n = 28) still perceived themselves as concerned and very concerned about social engineering attacks, and other participants (n = 34) reported a range of concerns about fraud ranging from moderately to slight (see table 6).

Table 6

Participants' Levels of Concern and Associated Narrative Insights

Level of Concern	**Concern Source**					*Total Mentio	**%
	Social Exposure	Personal Exposure[2]	Vigilance Against Fraud[3]	No Shared Source	Self-confidenc		
Very Concerned	2	3	4	1	-	10	12.65
Concerned	2	5	8	2	-	17	21.51
Moderately Concerned	8	8	4	6	-	31	39.24
Slightly Concerned	2	5	2	2	-	11	13.92
Not Concerned at All	1	-	-	4	5	10	12.65
***Mode	3.13	3.29	3.79	2.60	1	*n*=79	

Note. The total number of participants who reported their level of concern was 72. The total number of answers to the concern source was 61. The analyses were based on 79 entries, as some participants provided multiple sources of concern within a single response. **% represents the percentage of total mentions. ***The central tendency of sources appears most frequently within the data.

The findings align with previous studies that emphasize the role of individuals' feelings of unease about an issue, which often derive the decisions to behavior changes for the desired outcomes (Alston, 1969; Loewenstein et al., 2001; Winnicott, 1963). Furthermore, the analysis revealed that participants' narratives about incidents contributing to their concerns were not consistently aligned with the level of concern they reported. This suggests a complex interplay among fraud-related exposure, concerns about fraud, and confidence in adopting safe behaviors (see Table 6). However, the moderately concerned level appeared most frequently across all sources of concern about SEAs, with a total of 31 mentions. This indicates that participants with moderate concern reflected diverse fraud-related experiences and exposure. In light of the sources of concern, social exposure, where participants interacted with others who had harmful experiences with fraud, seemed to influence participants' levels of concern differently. For example, several participants who heard about and observed peers' negative encounters with fraud reported a wide array of concerns, ranging from very concerned to no concern. Similarly, participants who directly experienced attacks or engaged in suspicious interactions reported various concerns, as they described themselves as slightly concerned to very concerned. This trend of the wide range of concern was also noted among participants whose responses indicated they maintain vigilance against fraud and are aware of how scammers exploit advanced technology to deceive potential victims.

Conversely, a small subset of participants' responses (n = 10) conveyed a strong sense of confidence in their ability to recognize and avoid fraud attempts, leading them to report no concern about such attacks. Interestingly, what distinguished these participants is that, despite their confidence, they had experienced suspicious interactions with scammers, encountered fraud attacks, or engaged with other fraud victims. This pattern presents a compelling deviation from

the broader participant group, where similar fraud-related incidents appeared to heighten concern about the fraud risk rather than diminish it. Furthermore, since the primary goal of the current study was to explore the forms of communication and adaptation of secure action, it was important to identify which forms of communication contributed to participants' level of concern. For that, Table 7 below outlines the categories and subthemes related to participants' concerns about social engineering and the corresponding forms of communication.

Table 7

Subthemes and Categories of Participants' Sources of Concern and associated Communication forms

Subthemes	Categories	Examples	Number of references from the data
Interpersonal Communication (Close others)	Others' Negative Experiences with Fraud	الاستماع إلى الحوادث التي تحصل للكثير من الأشخاص (Hearing to the accidents that happen to many people)	12
		تلقى أحد زملاء السكن سرقة واحتيال (A roommate was robbed and scammed.)	
		A family relative lost some money from scammers.	
		سماع قصص عشوائية عن صرف المال بحسن نيه ثم استعماله بوسائل غير شرعية (Hearing random stories about money being spent in good faith and then used illegally.)	
Interpersonal Communication (Own)	Personal Negative Experiences with Fraud Personal negative Experience with Fraud abroad Suspicious Interaction	Steal my card information from shopping application.	28
		كثرة الاتصالات الهاتفيه ومعرفتهم لاسمي (Lots of phone calls, and they know my name)	
		توصلني بعض الرسايل المجهوله بتحديث العنوان او تاكيد العنوان على الرغم من صيغه بعض الروابط شبه حقيقيه (I receive some anonymous messages asking me to update or confirm the address, although some links' wording is semi-real.)	
		تم سرقة معلومات بطاقتي البنكية ولا اعلم السبب، "هذه ثاني مره تحصل لي هنا في الولايات المتحده. (My bank card information was stolen and I don't know why. This is the second time this has happened to me here in the United States.)	
		A message on my phone telling me to click on the link for Saudi Post.	
Perceived Invulnerability	Trust in Institutional Protection Participants' Self-Confidence	لست قلقا لان البنك هنا يوقف العملية ويسترد المبلغ إذا كان هناك عملية احتيال (I am not worried because the bank here stops the process and refunds the amount if there is fraud.)	5
		اكتسبت المهاراة التي تساعدني على ذلك *(I have acquired the skills that help me do that.)*	
		لست قلق، أعتقد لدي وعي كافي	

Intrapersonal Communication Exploiting Advance Technology	لا اثق في اجراء العمليات من خلال الاتصالات وافضل الذهاب للفرع مثل . البنك (I do not trust conducting transactions through calls and prefer to go to the branch like the bank.) *تطور طرق وأساليب الهجمات بشكل سريع.* (*Attack methods and techniques are evolving rapidly.)* مع تطور الذكاء الاصطناعي قد يكون الاحتيال المالي أسهل. With the development of artificial intelligence, financial	12

Note. The total number of answers to the concern source was 61. The analyses of associated responses with forms of communication were based on 57 entries, as some participants shared nonrelated responses or did not share at all, while others shared multiple sources of concern.

As presented in Table 7, the incidents that contributed to the concern about social engineering attacks, participants' concerns about fraud were not notably related to their situations abroad or their need to understand interaction norms in those settings better, as only a few participants reported encountering three fraud-related incidents while abroad, compared to other incidents that did not clearly indicate broad interaction, with 17 fraud-related stories and eight abroad incidents were the participants express their concern emerged from the of suspicious interactions with social engineering attacks (*interpersonal communication*). Further, participants determined that their concerns about fraud threats were influenced by various factors, including the fact that participants were vigilant about how scammers devolved their schemes, exploiting advanced technology with 12 fraud-related responses (*Intrapersonal communication*). Additional communication factors that shaped their fraud concern were based in their exposure to others' negative experiences, with 12 fraud-related stories (interpersonal communication).

To illustrate, the categories emerging from the participants' responses about fraud-related incidents contributing to their concerns were reflected in three subthemes highlighting various communication forms. The first subtheme derived from the answers was *interpersonal*

communication (close others), which included exposure to others' fraud-related stories. This exposure was based on participants' responses, either through direct conversation, hearing about incidents secondhand, or observing the consequences of fraud within their social circles. For example, hearing and observing others' stories influencing participants' concern about SEAs, one participant shared, "*سماع قصص عشوائية عن صرف المال بحسن نيه ثم استعماله بوسائل غير شرعية*" (Hearing random stories about spending money in good faith and then using it for illegal means.) Another participant added, "*الإستماع إلى الحوادث التي تحصل للكثير من الأشخاص خصوصاً على مواقع التواصل الاجتماعي*" (Listening to incidents that happen to many people, especially on social media sites.) Additionally, other participants reflected on the role of shared fraud stories through direct personal relationships in shaping participants' fraud concerns. For example, participants said, *"A family relative lost some money from scammers."* Another participant added, *"My father-in-law got a call from someone claiming to be my son asking for money."*

The second subtheme identified was *interpersonal communication* (own)—direct interactions with scammers through mediated channels such as emails, calls, and text messages. The subtheme includes participants who were victims of fraud, along with those who only had suspicious interactions, both of which were reported as incidents that contributed to participants' concerns about the risks associated with SEAs. Examples of harmful direct interaction with scammers included either financial loss or information leaks. As reported by, "*Steal my card information from shopping application.*" And "*Personal information leak, reputation damage.*" Another participant added, *"stalking my personal account and stealing information that is confidential."* Additionally*,* engaging in suspicious interactions, where no harm was reported, was also found to contribute to participants' concerns about the risks associated with the fraud. Based on the responses, the suspicious interaction encompasses incidents where participants

highlighted how scammers leverage social trust in specific entities and authority to deceive them into disclosing personal information. As reported in participants' responses, "*After finishing a call with Saudi Post, I receive a message on my phone telling me to click...*" and another participant added, "*رسائل الشركات للتحقق من حسابك او شيء كهذا*" (Company messages to verify your account or something). Thus, these responses highlighted trust exploitation that has contributed to participants' concern about fraud, in which scammers exploit various channels and advanced technology, such as suspicious calls and text messages. Given that trust in the government and other entities was one of the factors affecting Saudi users' information security (Alyahya & Weir, 2021; Alhasan, 2023), the findings indicated that Saudi students abroad were aware of such exploitation aimed at tricking them into disclosing information or taking action. As indicated by the data, participants' understanding of the way scammers leverage the trust in institutions and entities not only affects the participants' concerns about fraud but also encourages them to be more secure, such as sample, "*في السعوديه وخارجها من مكالمات تدعي انها جهات حكوميه موثوقه*" (In Saudi Arabia and abroad, calls claiming to be from trusted government agencies.) Another participant shared, "*قد يحتالون على كبار السن بطرق احتيال مختلفة بإيهامهم بانهم جهة رسمية*" (They may scam elderly people through various fraud methods by deceiving them into believing they are an official entity.)

The third subtheme identified was *intrapersonal communication*; these responses reflected participants' internal reflections and vigilance in recognizing sophisticated fraud tactics. Notably, the responses demonstrated that participants' concerns about fraud risk were closely linked to their understanding of how scammers exploit advanced technology, including concerns about fraudulent websites and artificial intelligence. For instance, participants mentioned that "*The advancement in AI technology made some videos or messages seem very*

believable," and another student added, " *الاحتيال المالي اسهل من الممكن استخدام الذكاء الاصطناعي لتعرف على بصمة الوجه او الصوت*" (Financial fraud is easier as it become possible to use artificial intelligence to recognize a face or voice fingerprint). These responses demonstrated the participant's distrust in digital tools, particularly the IA that powered the attackers' schemes, such as deepfake videos and voice cloning, making scams more convincing and harder to detect. These responses demonstrate the growing vigilance considering the advanced fraud techniques contributed to participants' fear and vulnerability in identifying scams, such as one participant said "*تحديث طرق الاحتيال و اختلافها في كل مرة عن المرة السابقة*" (Updating the fraud methods and making them different each time from the previous time) and another participant added " *الان اصبحوا يستحدثون حيل جديدة واحترافية للاحتيال. اخاف ان اكون اجهلها*" (Now they are coming up with new and professional fraud tricks. I'm afraid I don't know them.). As noticed in participants' responses, the internal evaluation of the potential risks was often triggered by thoughts and feelings, particularly fear and suspicion, as one participant stated, "*لأن الأمور السيئة قد تحصل*" (Because bad things can happen). Another shared that " *إدخال معلومات البطاقة البنكية في المواقع المختلفة سواء المشكوك بها او الموثوقه يثير قلقي قليلا*". These emotional responses seemed to drive the adoption of protective behaviors as participants became more vigilant of the risk associated with SEAs. For example, one participant said, "*We need to be careful all the time,"* and another participant said that " *لا اثق في اجراء العمليات من خلال الاتصالات وافضل الذهاب للفرع مثل البنك او شركة خدمات خاصة*" (I do not trust conducting operations through calls and I prefer to go to the branch).

Conversely, several students (n = 10) reported not being concerned about the risk associated with SEAs, highlighting their confidence that they are likely to be able to avoid such a threat. Based on the participants' stories, participants who were not concerned at all had specific attitudes toward having sufficient knowledge to protect themselves from social engineering

attempts. For instance, " *لدي المقدرة الكاملة للتعامل مع الهندسة الاجتماعية" وخاصة في اكثر من موقف في بريطانيا تم ردعهم بكل بساطة*" (I have the full ability to deal with social engineering," especially in more than one situation in Britain, where they were simply deterred.) another participant said, " *لست قلق أعتقد لدي وعي كافي*" (I'm not concerned, I think I have enough awareness). Only one of these participants has highlighted that confidence in institutional protection lowers the concern about fraud risk, as this participant said: "*لست قلقا لان البنك هنا يوقف العملية ويسترد المبلغ إذا كان هناك عملية احتيال*" (I am not worried because the bank here stops the process and refunds the amount if there is a fraud.). These responses of confident participants were grouped into two categories: *participants' self-confidence* in avoiding fraud (n = 4) and trust in institution protection (n=1) (see Table 7). Self-confidence and institutional trust categories were then incorporated into the subtheme referred to as *perceived invulnerability,* in which participants believe they have developed sufficient skills to reduce anxiety about SEA.

RQ2: *What forms of communication encouraged Saudi Arabian students abroad to take secure behavior to protect themselves from SEA?*

The second research question was investigated using data obtained from participants' responses to questions 3, 4, and 5 of the survey (see Appendix A). Although these survey questions did not explicitly ask about the incidents that led to the adoption of secure behaviors, the current study suggested that memorable stories are more likely to contribute to shaping the concerns and recognition against SEAs. As previously discussed, drawing from the theory of memorable messages, prior research has explored how these memorable messages influence people's cognitive, emotional, and behavioral responses (Anderson et al., 2020; Cooke-Jackson & Rubinsky, 2023; Kuang et al., 2023; Smith et al., 2009). To further strengthen this connection, the current analysis revealed that the fraud-related stories in these questions correspond with participants' responses, which showed whether communication forms influenced their concerns

regarding social engineering threats. The analysis of participants' most memorable fraud-related stories is detailed in the following data (see Table 8).

Table 8

Subthemes and Categories of Memorable Fraud-Related stories and associated Communication

Subthemes	Categories	Example Participant Responses	Number of references from the data
Interpersonal Communication (Own)	Personal Negative Experience with Fraud	Someone emailed me and exposed my password.	26
		I experienced fraud when I bought a coupon	
	Personal Negative Experience with Fraud Abroad	I received a call from someone claiming to work for SACM in the US	16
		Never ever experienced such thing in KSA no one at all ever asked me for my card credentials	50
	Suspicious Interaction	Selling furniture in the Facebook. The buyer insisted to exchange a code.	
Interpersonal Communication (Close other)	Others' Negative Experiences with Fraud	My brother wanted to invest in stocks...	53
		One my friends access a fake bank website	
		A university dean's WhatsApp account was hacked	
		I have seen older people become victims of scams	
Intrapersonal Communication	Exploiting Advance Technology	الاحتيال متطور وله أساليب متعددة ويجب مواكبة ذلك (Fraud is sophisticated and has multiple methods and must be kept up with.)	6
		التطبيقات المتداولة وانتقال صفحاته بغرض خصومات او عروض وهمية (Commonly used apps and navigating their pages for fake discounts or offers.)	
		Afraid to be behind on technology and recognize the	
Institutional Communicatio	Authority Warnings	المؤثرين في مواقع التواصل الاجتماعي التي تحاول أن تنشر الوعي وتحذر الناس. (Social media influencers trying to spread awareness and warn people	18
	Media Messages	The media always has some people warning us about the new ways that attackers	
	Social Media Posts	رسائل البنوك بعدم مشاركة معلوماتي (Bank messages not to share my information)	

Note. The total number of answers to fraud-related incidents was 167. The analyses of associated responses with forms of communication were based on 169 entries, as some participants shared multiple incidents within a single response.

As presented in Table 8, the participants contributed 169 responses, these fraud-related references reflect the number of reported stories rather than the number of individual participants, considering that several participants were able to recall multiple incidents within a single response. These responses showed that participants have either learned about the fraud risk or been exposed to others' fraud-related stories and are more likely to influence their concern about SEAs and adopting secure actions. The analysis revealed that participants were able to recall stories about situations involving fraud, reading to identify several memorable forms of communication. Based on the analysis, shared fraud-related stories with close others, including family, friends, and acquaintances (*interpersonal communication (close other*) (*f* = 53), along with participants' suspicious interactions with scammers (*interpersonal communication (own*) (*f* =50)—whether in Saudi Arabia or abroad—all of which were among the most common memorable forms of communication.

This was followed by participants who shared their harmful fraud stories (*interpersonal communication (own*) (*n*= 42). These direct interactions with scammers—primarily through mediated communication, including scam calls, emails, and other digital platforms- were also memorable and more likely to motivate participants to be more cautious about avoiding SEAs. Following these forms, *institutional communication* was also identified within participants' responses, including media messages, authority warnings, and social media posts, with 18 related responses. Additionally, *intrapersonal communication* was determined, in which participants expressed their concern (emotional reactions) about the advanced technology scammers exploiting for malicious attacks, which appeared to be the least form that emerged in

participants' responses, with six related responses. To illustrate, a notable distinction in the data was found in the participant's interpersonal interaction with social engineers. *Interpersonal communication (own),* similar to the findings in RQ1, these interactions were divided into two experiences. First, it represents incidents where participants experience harmful fraud attacks; in other cases, participants encountered fraud but noticed the red flags and managed to avoid it (suspicious interactions). These direct interactions with scammers primarily occurred through exploited mediated communication channels like emails, text messages, and online applications. Examples of stories in which participants experience harmful fraud attacks include, "*I paid for a printer from Instagram advertisement and they stole my money*", and another participant shared, "*An amount was withdrawn from my account*."

Other non-harmful interactions with scammers were seen in stories like, "*I almost get a call every day claiming a potential government loan*." Another participant added, "*One phone call was trying to know what electricity provider I'm with.*" These direct interactions were memorable and likely encouraged participants to adopt more secure behaviors to avoid scams facilitated by technological tools and digital platforms. Considering participants navigating less familiar interactions, 26 of these interactions did not explicitly indicate whether they occurred while abroad, whereas 16 incidents were confirmed to have taken place while participants were in Western countries. This suggests that participants' unfamiliarity in navigating interaction in a new culture—such as different communication norms or financial systems—may have heightened their vulnerability to fraud. For example, one participant mentioned, " *كطالب في أمريكا، أشاهد وأتعرض لمحاولات كثيرة للاحتيال المالي، خصوصاً عند الرغبة ببيع أو شراء سلعة معينة* بشكل شخصي. (As a student in the U.S., I frequently encounter and am exposed to various financial fraud attempts, especially when trying to buy or sell an item in person.) Another participant added, "*I received a*

call from someone claiming to work for SACM in the US & telling me I have pending fees."

The second subtheme identified was interpersonal communication (close others). These responses demonstrated the participants' ability to recall fraud-related stories shared through conversations with family and friends and hearing about incidents secondhand, with 46 instances noted. These narratives emphasize the role of interpersonal interactions within social circles in influencing participants concerned about fraud and reinforcing protective measures. For example, one participant shared, "*A lot of friends or mutual friends been in this experience."* Another participant added*, "Many friends unfortunately fell to those scams".* Further, shared fraud stories also included hearing or observing fraud-related experiences involving individuals beyond their immediate circle, such as viral stories on social media and acquaintances. This observation drawing from participants' answers like, "*I have seen older people become victims of scams*" and "*سمعت عن طرق احتيال مثل تحديث بينات بنكية عبر روابط وهمية*" (I heard about fraudulent methods, such as updating bank information via fake links.). These responses indicate that emotional and personal connections with fraud victims may be more likely to be memorable and may encourage safer actions, as reflected in responses like, "*My father was tricked by a scammer*" and "*My closest friend has been given a fake opportunity."*

The third subtheme focused on intrapersonal communication. Responses in this area reflect participants' concerns and their evaluations of the advanced technology that scammers might exploit, especially the potential misuse of digital tools to deceive individuals into revealing personal information. These were drawn from participants' responses like, "*Afraid to be behind on technology and recognize the scams*." While another mentioned being "*Not familiar with the technology."* Such responses highlighted the participants' recognition of malicious activities used to deceive others, including exploiting technology and misusing digital tools, such as callers

impersonating legitimate entities, suspicious emails, or fraudulent messages. More responses in this regard include, "*الاحتيال متطور وله أساليب متعددة و يجب مواكبة ذلك برفع الأنظمة الأمنية*" (Fraud is evolving with various sophisticated techniques, and it is essential to keep up by enhancing security systems.) Thus, participants' ability to express their internal concern about the fraud risk and evaluate potential threats may have heightened their vigilance to adopt safe behavior to defend themselves against possible threats.

The last subtheme identified was *institutional communication*, comprised of respondents recalling and sharing fraud-related information received via media and public warnings, with a total of 18 responses. Based on the responses, these institutional messages were delivered as references from the data, which included nine mentions of viral stories on social media, four references to fraud-related news content, and five warnings issued by authorities. These were shared as memorable stories and served as sources of information that contributed to general awareness about scams and offered guidance on prevention practices. Although the institutional communication forms were less prominent in the responses, they served as essential channels for delivering educational materials aimed at influencing secure behavior adaptation. Drawing from the data, participants highlighted those negative stories shared on social media, often through influencers or public posts, had influenced their recognition of scam activities and the potential threats they might face. For example, one participant said, "*A lot of disappointing stories in the social media*," while another shared, " *المؤثرين في مواقع التواصل الاجتماعي التي تحاول أن تنشر الوعي وتحذر الناس.."* (Influencers on social media who try to spread awareness and warn people). Another participant said, "حسابات التواصل ودايما يحذرون وبنشرون منشورات توعوية حول ذلك" (Social media accounts always warn and publish awareness posts about this.)

Furthermore, other participants have indicated that public campaigns have highlighted the

risks associated with fraud, as reflected in responses such as, "*I have noticed that government agencies frequently announce,"* another participant mentioned, "*the media always has some people warning us about the new ways that attackers*." Along with responses like "*government agencies frequently announce.*" and "*The news is filled with stories,*" Although mentioned less frequently, these responses underscored the crucial role of institutional messages in delivering educational content and raising awareness about fraud threats. Mass communication often reiterates messages; this principle is central to mass communication strategies to enhance familiarity and recall (McQuail, 2010; Schramm, 1954). In this context, repeated exposure has been found to shape attitudes toward an issue, leading to increased awareness, particularly when individuals lack the motivation to engage with the content. (Harmon-Jones & Allen, 2001; Zajonc, 1968). Consequently, these repeated messages from institutional communication seemed to enhance their memorability and potential impact on participants, particularly regarding such threats. This finding aligns with the forms of institutional communication identified in RQ1, which refer to messages from institutions, authorities, and the media.

RQ3: *In what ways did a key message (e.g., cultural, religious, content, sources) influence participants to take protective behavior against fraud in unfamiliar environments?*

The third research question specifically addressed how a message influences the decision to take secure behaviors against social engineers' attacks. This question aimed to identify which types of memorable messages have impacted the decision to take steps to protect themselves from fraud attacks and whether a key message is commonly recalled by Saudi students studying abroad who are participating in the current study. The data were derived from the narratives of 55 participants responding to free-response questions 6 and 7 of the survey, who recalled 99 influential messages according to participants (see Table 9). Based on the analysis, participants were able to recall various messages related to secure behaviors. Table 9 presents the categories

and subthemes of memorable message types reported by participants, as well as their frequencies in the data.

Table 9

Subthemes and Categories of memorable messages contributed to behavior change.

Subthemes	Categories	Example Participant Responses	Number of references from the data
Intrapersonal Communication		The law does not protect the foolish.	
	Culturally Inspired Wisdom	A true believer is not bitten from the same hole twice.	20
		No one can ride your back unless you bend	
	Avoidance Strategy	Always check email address before responding	60
		Avoiding writing my email for links send directly to me.	
		Checking URL's.	
		Don’t believe who is rushing you or make you in a fear or excitement.	
Institutional Communication		حملة (خلك حريص) من المصارف السعودية (Be careful) campaign from Saudi banks)	
	Authority Warnings	رساله البنك التي تذكر العملاء بأن البنك لايطلب معلومات شخصيه.	10
	Media Messages	Bank messages remind customers that the bank does not ask for personal information.	5
	Academic Instruction	مقاطع الفيديو التي ينشرها بعض المؤثرين في مواقع التواصل الاجتماعي.	1
		Videos posted by some influencers on social media.	
		في جامعتي ترشدني عبر فيديوهات تمثيلية قصيرة أكملت دورة تدريبية مجانية online عن أنواع الاحتيال المختلفة I completed a free online course at my university that involved watching short video demonstrations of different types of fraud.	
Interpersonal Communication		العظة والعبرة من تجارب الاخرين. The lessons learned from the experiences of others.	3
	Other’ Negative Experiences with Fraud	مواقف الاصدقاء Friends’ stories	
		الحوادث والقصص التي نسمعها The incidents and stories we hear	

Do not Remember	Nothing in particular (Nothing to say) لا يوجد (I do not remember) لا أذكر	14

Note. The total number of answers to fraud-related memorable messages was 96. The analyses of associated responses with memorable messages were based on 99 entries, as some participants shared multiple messages within a single response while others shared unrelated contexts.

As presented in Table 9, participants remembered 33 messages containing various avoidance strategies they used to protect their information, 18 wisdom-based messages, six warning messages issued by authorities, four messages from media, and only one mention of information introduced through a training program. Whereas, 14 participants reported not remembering any messages that had influenced their secure behaviors despite expressing concern about fraud and actively using secure actions. Furthermore, when participants were asked to identify the most compelling messages related to avoiding social engineering attacks, they predominantly highlighted their avoidance strategies as the most influential in enhancing security against fraud. This was by sharing additional 27 messages focused on actionable steps to protect personal information from these attacks. Other participants emphasized that warning messages from media were particularly impactful, while three participants highlighted the influence of peers' stories involving scammers, and only two mentioned that words of wisdom compelled them to adopt secure behavior. These findings may be biased toward specific types of messages since respondents were provided with examples aimed at triggering their memory, including logos, signs, comments, phrases, or words of wisdom.

As an illustration of the findings, the most commonly reported type of memorable message was *avoidance strategies*, such as practical steps and actionable advice for fraud prevention, with 60 specific avoidance strategy messages recalled. Based on the responses,

actionable advice mainly refers to participants' sense of cautiousness and behavioral reactions to avoid potential threats; for example, participants' answers like, "*My money shouldn't be accessible to scammers,*" and another mentioned, "*the less you share, the more safe you are."* While the practical steps refer to participants' readiness to recognize threats and act carefully. These responses involve concrete guidance to avoid fraud attempts, as reported in participants' responses: "*Call yourself and check out everything*" and *"Never pay for anything before checking if the product actually exists."* Building on previous studies that examine memorable messages and behavior change (Cooke-Jackson & Rubinsky, 2021; Kumaraguru et al., 2007; Waldron et al., 2023), the current findings emphasize the importance of providing practical anti-fraud messages, such as step-by-step guidance for identifying and avoiding social engineering attacks. This is particularly crucial for students studying abroad, who often face challenges in navigating unfamiliar interactions.

Furthermore, messages that included concrete action steps were the most compelling because these steps offered immediate tools for participants to avoid security threats in less familiar interactions. Examples of memorable and influential messages were those that emphasized practical steps, such as one participant shared, "*If the website doesnt have the lock icon in the url bar, dont even review it."* another student added, "*إذا مرجع الاتصال او الرساله برقم دولي خارجي"* (If the call or message refers to an international number). Additionally, actionable advice as memorable messages has been observed to reflect participants' emotional reactions, such as feelings of suspicion and distrust. Adopting that attitude also seems to influence secure behaviors aimed at preventing victims from failing scams, as one participant reported, "*Always pay attention, as they will find new ways to access your personal information."* Another participant said, *"الانتباه لكل ما يرد الينا من ايميلات غير معروفة لدينا و عدم تصديقها"* (Pay attention to all emails from

unknown senders and do not trust them.) These responses were placed in the avoidance strategies category, where participants expressed their emotional states and associated behavioral responses to secure personal information.

The second category found among the reported memorable messages was culturally inspired wisdom. This arises from participants' cautiousness and self-responsibility toward safely protecting their confidential information. Drawing from the responses, "*No one can ride your back unless you bend,*" another participant said, "*The law does not protect those who are careless.*" Such responses reflect the participants' internalized attitudes against SEAs, such as skepticism and concern (emotional responses), which might motivate them to take security measures to avoid fraud (behavioral responses). For most respondents, culturally inspired wisdom messages were more likely to be derived from both general beliefs as well as Arab cultural norms and religious contexts. This finding provides further insights into how memorable wisdom-based messages served as guides that influenced behavior, highlighting their role in motivating participants toward cautious attitudes and proactive practices that favor legal and financial matters in foreign countries beyond Saudi and Islamic cultures. As evidenced by the respondents, the broad side of these sayings represents common principles such as using caution and personal responsibility to guide secure behavior. While other wisdom-based messages were also deeply rooted in Arab culture and Islamic teaching, which reflected traditional values of generosity, accountability, and moderation in financial behaviors. As examples from the data, the English proverb "*Fool me once shame on you, fool me twice shame on me*" conveys a similar meaning to the Islamic saying "*لا يلدغ مؤمن من حجر مرتين*" (A believer is not stung from the same hole twice). Both sayings showed the participant's internal emotion and cognition to be more cautious and responsible for avoiding mistakes as well as learning from past experiences.

Furthermore, the data revealed that participants had established the responsibility to protect themselves from scam attacks abroad. This finding presents a complementary perspective compared to prior studies emphasizing Saudi citizens' expectation that authorities are primarily responsible for information security (Alarifi et al., 2012; Alzubaidi, 2021). Based on the data, wisdom-based messages influencing participants have emphasized their vigilante and responsibility against social engineering threats, ensuring that participants appeared prepared to navigate less familiar environments securely. Such findings can be seen in participants' responses like, "*Don't share what you wouldn't want the world to know*" and"*القانون لا يحمي المغفلين The law does not protect the foolish,"* reflecting a sense of personal responsibility particularly in financial matters. Such responses suggested that participants recognized fraud risks and the importance of caution and self-accountability, especially in protecting themselves from these threats. This finding indicates that participants may alter their approach to security, showing a tendency for increased vigilance against fraud compared to cultural norms in Saudi Arabia, which emphasize trust and sharing. These cultural norms have been shown to contribute to Saudi users' vulnerability to fraud threats (Al-Ghaith, 2015; Alyahya & Weir, 2021).

Additionally, by challenging the focus of prior studies, this study brings attention to the role of social trust in shaping Saudi users' information security (Alhasan, 2023). The current data demonstrate that participants have exhibited reduced trust and heightened caution in safeguarding their information, suggesting a shift in behavior influenced by their experiences in less familiar interactions. For instance, one participant said, *"Scams thrive on trust,"* while another mentioned, "*To not trust the social media that portrays a safe website."* Moreover, one participant added, *"الاختراق قد يأتي من قبل أشخاص يدعون بمعرفتك"* (The hack may come from people who claim to know you) and another participant added, "*Trust no one for confidential*

information over a phone call or message." These answers highlighted the participants' thoughts and emotional reactions regarding fraud, such as distrust. This distrust reflected their behavioral responses to protect themselves from potential threats, indicating that trust seemed to have no effect on their security awareness while abroad.

The third category, *institutional communication*, consisted of five responses to media content and ten authority warnings, shared as memorable and influential messages in encouraging participants to take protective measures against fraud threats. As reported by participants, "*إشعارات بنكية استقبلها بين الحين والآخر تحذرني*" (I received bank warnings from time to time warning me.) One participant also said, "الرسائل المتكررة *من الجهة المعنية مثل الاتصالات والبنوك*" (Repeated messages from the concerned authority, such as telecommunications and banks). Furthermore, as drawing from participants' input, for example, *'' مقاطع الفيديو التي ينشرها بعض المؤثرين في مواقع التواصل الاجتماعي*" (Video posted by some influencers on social networking sites). Another participant mentioned they "*follow people who are always sharing and exposing the new scamming tactics*." With limited participant input, these responses highlighted that exposure to institutional fraud-related content has influenced participants' engagement in safer behaviors over time. According to the respondents, these messages enhanced their recognition of scammers' tactics and encouraged them to engage in fraud-prevention practices. This finding broadens the scope of memorable messages, highlighting the influence of institutional communication and message repetition on impact and memorability, particularly when these messages come from trusted sources, such as the Saudi government, social media influencers, and local Saudi banks, directed at Saudi citizens.

In alignment with that, participants also reported that conversations with family and peers were memorable and influential in encouraging them to adopt secure practices. For instance,

participants said that hearing others' stories and personal connections with close others who were fraud victims were memorable and motivated them to adopt safe practices, such as *" العظة والعبرة من تجارب الاخرين"* (The lessons learned from the experiences of others) another participant mentioned that *"الحوادث والقصص التي نسمعها"* (The incidents and stories we hear). While conceding the exploration of memorable messages, it is noteworthy that shared experiences from close others who were fraud victims had minimal representation, with only three reported responses seen as compelling messages encouraging secure behaviors. These responses were notably prominent in participants' answers to other survey questions regarding memorable fraud-related incidents, emphasizing the influence of social interactions and interpersonal communication against SEAs.

RQ4: *In what ways are memorable messages and taking secure behaviors linked among Saudi students abroad?*

To address RQ4, the researcher observed all the participants' responses, including their memorable messages, recollections of direct interactions with fraud, secondhand stories from others, and internal reflections on fraud risks. These can be seen as memorable communication events associated with participants' concerns about SEAs and promote secure behaviors. Based on the data, the current study found that participants recalled various forms of memorable interactions and different types of memorable messages, as introduced by Knapp and Reardon (1981). As presented in Table 10, the current study analysis revealed that participants, with respect to the variation in the amount of evidence, have recollected fraud-related stories of others (interpersonal communication (close others), their direct experiences with fraud (interpersonal communication (own), expressing their internal emotional and behavioral responses against SEAs (intrapersonal communication) as well as remembering messages delivered through a

medium (institutional communication)—where they encountered content related to social engineering attacks. Notably, most of the reported memorable interactions occurred through interpersonal communication, with 188 incidents happening within participants' social circles and direct exposure to scammers. Following that was intrapersonal communication through both participants' emotions about fraud risks (concerns) and behavioral responses (secure actions), with 120 internal reflections on their recognition and readiness to protect themselves. Additionally, participants recall 37 responses highlighting institutional communication, all these responses collectively highlighted participants' recognition of the threat associated with SEAs and explained the multiple secure actions they take to defend themselves against social engineering attacks in less familiar interactions. Thus, the current study suggested that the memorability of messages and secure behaviors among participants are linked through the communication events presented in Table 10.

Table 10

Themes and Subthemes of memorable messages and taking secure behaviors

Themes	Subthemes	Description	Number of references from the data	%
Interactivity in Fraud Awareness	Interpersonal Communication (Close Others) Interpersonal Communication (Own) Intrapersonal Communication	This theme highlights the role of interactive elements in enhancing the memorability of stories related to social engineering attacks and shaping participants' concern and recognition of such risks.	308	89.27
One way-communication	Institutional Communication	This theme includes participants' responses that recall fraud-related messages conveyed through mediums like universities, authorities, and media, influencing their concern and recognition of such risks.	37	10.72
			F = 345	

Note. Memorable messages included the various forms of communication that contribute to participants' concern and recognition of social engineering threats.

The dynamic interplay in interpersonal communication—through conversations with close others and interactions with scammers—as well as intrapersonal communication, which involves participants' internal dialog reflecting in their emotional evaluation and behavioral responses to the fraud threat, have appeared to shape participants' ability to recognize fraud and their secure behaviors. This interaction, combining external conversations and internal cognitive responses, enhances the memorability of fraud-related information and reinforces cautionary behaviors, particularly in less familiar environments. However, institutional communication appeared to be less memorable in participants' responses. This suggests that fraud-related messages from institutional sources may not be as impactful or memorable as those from interpersonal and intrapersonal communication, likely due to the more passive nature of message processing, where participants received information without actively engaging in an exchange.

Summary

This chapter presents the findings of a qualitative exploration study. The findings focus on understanding the lived experiences of Saudi students abroad and whether communication methods are linked to their concerns and secure behavior regarding SEAs in less familiar interactions. The purpose was fulfilled through data collected from 72 purposive selected Saudi students currently enrolled in universities in Western countries. Data collection was conducted through an online open-ended survey. The data analysis process was followed the inductive qualitative content analysis to identify recurring themes and patterns throughout the analysis, enabling the researcher to recognize repetitive keywords and similarities (Hsieh & Shannon, 2005; Thomas, 2006). The findings revealed two themes reflecting the participants' unique stories and experiences that addressed the research questions. The themes included "interactivity

in fraud awareness" and "one-way communication." The next section briefly summarizes these themes along with their associated subthemes as they emerged from the data.

Theme one: Interactivity in Fraud Awareness

The interactivity in fraud awareness themes was identified from the responses in three subthemes reflecting participants' interpersonal communication either with close others or with scammers, as well as participants' intrapersonal reflection reflecting participants' emotional reactions and the behavioral responses. The interaction in fraud awareness feature in the current study refers to the different ways participants exchange and process fraud-related information, including direct encounters with scammers, where participants either fall victim to fraud or experience suspicious interactions with scam attempts. Additionally, the interactions include situations where participants conversed with and witnessed others who had fallen victim to fraud, mainly within the participants' social circle. Based on the responses, this interaction was found to be crucial for understanding how participants become motivated to act more cautiously, emphasizing the significance of personal relevance, emotions, and interest in engaging with it. This was suggested from the detailed stories provided by participants who shared their fraud-related stories involving responses occurring within the interpersonal and intrapersonal communication events. This highlights the way these communication events and interactions with fraud-related have enhanced the storing and recalling of related information more effectively.

Subtheme: Interpersonal Communication (Close Others & Own)

Previously, researchers indicated that interpersonal interaction with peers and family has a considerable impact due to the personal and emotional connections involved (Dunleavy &

Yang, 2015; Lucas & Buzzanell, 2012; Kaufmann et al., 2021). The current study similarly found that personal experiences and interactions with scammers, even when participants were not victimized during those interactions, have appeared to be associated with participants' recognition of the fraud risk and the need to behave more cautionary. Drawing from the participants' input, "*This experience made me realize how easily people can exploit social media to manipulate others."* another participant said, "*After that I was aware of these messages, so I'd report it everytime."* One participant mentioned, *"I'm the target of these attacks in weekly basis through phone and emails but the solution is to block them".* The relationships established during fraud-related incidents enhance the memorability of these events, both personally and emotionally; this underscores how individuals process information more deeply, making it more memorable and more straightforward to recall.

This idea draws upon participants' detailed narratives of incidents that occur through indirect communication events, where secondhand stories are conveyed involving individuals beyond their immediate circle, such as mutual friends and acquaintances. For example, one participant response with details, " *اخبرني احد الاصدقاء، ان زوج اخته دكتور , , واذا به محتال وقد انتحل شخصية احد اعضاء . . . الخ."* (A friend told me that his sister's husband was a doctor, and then he met a fraudster who impersonated a member. . . .etc.) another participant added "*A university dean's WhatsApp account was hacked, and a link with a strange address was sent out.. . .etc.).* These narratives were not fully presented to maintain participants' confidential information and identity. Drawing from behavioral science, the current study interprets the interactions between individuals—whether with scammers or others fraud victims—which motivate active engagement, such as responding to conversations and triggering emotional states like fear and anxiety, leading to behavioral changes to address these threats (Burkhardt, 1994; Lewis et al.,

2006; Ploderer et al., 2014). In protective behavior, the connection between individual interactions and memorable communication indicates that they can enhance relevant knowledge and heighten the risks associated with such threats, thus facilitating individuals' ability to remember and act on safe behaviors. This highlights the significance of individual interactions in not only increasing the memorability of these incidents but also actively shaping secure behaviors.

Subtheme: Intrapersonal Communication (Protective Attitude)

Based on the data, intrapersonal communication emerged as participants reflected on their internal emotional reactions, such as fear and suspicion, and the resulting behavioral responses. These encompass categories reflecting participants' vigilance against fraud, recognition of scammers' use of advanced technology to deceive potential victims, adoption of strategies to prevent potential attacks, and a sense of responsibility for maintaining secure practices. These appeared to influence participants' sense of caution and ability to adopt secure behavior. To illustrate this point, participants expressed their vulnerability to potentially becoming fraud targets and their recognition of the risks associated with social engineering attacks, both of which have helped them develop a mental framework that enhances remembering fraud-related knowledge. Drawing from participants'' input that highlights this idea including, "*لكن فكرة الذكاء الاصطناعي ممكن يكون اهم العناصر مساعدة في الاحتيال المالي خلال الفترة القادمة*" (But the idea of artificial intelligence may be the most important element to help in financial fraud during the coming period.) other students added, "*لأن الأمور السيئة قد تحصل*" (Because bad things might happen.) and "*الان اصبحوا يستحدثون حيل جديدة واحترافية للاحتيال. اخاف ان اكون اجهلها*" (Now they are coming up with new and professional fraud tricks. I'm afraid I don't know them.). Further, to highlight the participants' emotional reactions, such as feeling suspicious and fear in

less familiar interactions, contributed to not only recalling related messages but also their responses to be take secure actions, this idea, as participants noted, " *فـي كل موقف ابحث امكانية الاحتيال في هذا الموقف واتجنب جميع الثغرات الممكنة مع مزيداً من التحيط*" (In every situation, look for the possibility of fraud in this situation and avoid all possible loopholes with extra caution.) " *أن الشخص لابد يكون حريص حتى لا يستغفل وينطلي عليه الاحتيال من أي مكان أو بأي أسلوب*" (A person must be careful not to be fooled and deceived by fraud from anywhere or in any manner). This aligns with the idea of attitudes toward the behavioral outcome introduced by Fishbein and Ajzen, 1975—specifically, in the current study, a positive attitude toward threat-reducing behavior appears to contribute to adopting secure practices. These protective attitudes reflect participants' vigilance and willingness to engage in secure practices against social engineering attacks. Protective attitudes are reflected in participants' emotional awareness of fraud threats and perceived vulnerability to fraud risks, influencing their vigilance against fraud and enhanced recall of fraud-related knowledge.

Theme Two: One-Way Communication

This theme is reflected in the participant's responses included in the subtheme of institutional communication, though supported by limited evidence, presented to highlight the role of one-way communication events influencing participants' recognition of the fraud threats and ways to avoid it. This emphasized the unique efforts of the government and institutions to educate the public about the threats associated with social engineering attacks. When comparing the one-way communication theme with the interactivity in fraud awareness identified in the data—interpersonal and intrapersonal communication—it becomes clear that participants' contextual and psychological factors influence the challenge of recalling fraud-related messages.

Several studies indicate that individuals tend to remember incidents that hold personal relevance, as participants recall communication events within their social circles involving family and friends (Harris et al., 2018; Petty & Cacioppo, 1986). Conversely, participants were less likely to retain messages from institutional communication due to a lack of motivation and relevance. This discrepancy became clear when participants could easily remember specific and detailed stories shared during social interactions compared to the general information presented by one-way communication tools. For example, participants mentioned answers such as "*News*," "*Media*," "*الاغلب من قصص التواصل الاجتماعي*" (Mostly from social media stories), and "*الرسائل الموجهة من شركات الاتصالات والبنوك*" (Messages sent from telecommunications companies and banks). The data indicate that while participants recalled institutional messages, they did not provide specific information, as seen in the other responses in other subthemes. Consistent with previous research, when passively consumed, mediated messages can be more challenging to remember as they often lack the emotional relevance and engagement necessary for effective memory retention (Lang, 2000; Phelps, 2004).

Although risk-awareness messages are designed to evoke emotions in individuals, particularly fear and a sense of threat (Moussaoui et al., 2021; Whitmer & Sims, 2023), the current findings revealed that participants were less likely to remember mediated messages compared to other messages shared and experienced through interpersonal interactions. These findings highlight the key elements of memorable communication events in risk-based messages and the factors influencing participants' information storage and recall processes. Notably, the relational context in which messages are exchanged—during social and personal interactions—plays a crucial role in enhancing memory recall, highlighting the importance of interactivity in fraud awareness. Additionally, participants' attitudes, including their positive stance toward

threat-mitigating behavior and their underlying values, further enhance the storing and recalling of such messages. These findings were interpreted and discussed in the discussion chapter. The following chapter also includes the implications, recommendations, as well as the limitations identified throughout the study.

CHAPTER 5: DISCUSSION

Overview

Social engineering attacks are rapidly increasing, exploiting individuals' psychological vulnerabilities, cultural factors, and technical gaps to manipulate them into disclosing sensitive information such as banking details and verification codes (Hadnagy, 2010; Steinmetz et al., 2020; Thomas, 2002). Fraudsters continuously refine their tactics to take advantage of emerging vulnerabilities, allowing them to stay ahead of detection efforts (Steinmetz et al., 2020; Talib & Rusly, 2015). Social engineering threats were often regarded as technical issues, focusing on identifying gaps in tools and detection measures (Hadnagy, 2010; Milletary & Center, 2005). However, as the nature of these threats has evolved, the emphasis has shifted toward individual behavior, which plays a crucial role in avoiding such threats, making public awareness of these sophisticated tactics essential for protecting people from such threats to their information (Alhasan, 2023; Ceesay et al., 2018; Schneier, 2000). Therefore, it is valuable to explore the communication factors influencing individuals' fraud concerns and protective behavior, mainly focusing on whether communication forms and memorable messages contribute to shaping recognition and behavioral responses against SEAs.

Identifying communication events and memorable messages that influence individuals' behavior against social engineering attacks contributes both to enhancing risk communication strategies and to expanding theoretical knowledge related to message effects and behavioral change theories. Considering that social engineers exploit individuals' vulnerabilities (Atkins & Huang, 2013; Michel & King, 2019; Workman, 2008), international students, especially Saudi students in unfamiliar environments, may face increased fraud risks due to cultural differences, language barriers, and financial systems (Alsanea, 2023; Hofer, 2009; Heyn, 2013). This

qualitative study aimed to explore how memorable communication events and messages influence Saudi students in Western universities to adopt secure behaviors against social engineering attacks. The main objective was to identify communication events in fraud-related stories shared by Saudi students that enhance message retention and promote secure behaviors against SEAs in these interactions.

The current chapter discusses the study's findings, including a synthesis of these findings an in-depth discussion of the subthemes and themes resulting from participants' fraud-related stories and experiences. This is followed by a discussion of the study's limitations and recommendations for future studies on memorable communication and secure behavior. The chapter then examines the findings' implications for risk communication, fraud prevention strategies, and behavioral change frameworks. Lastly, the chapter summarizes the main findings and conclusions, emphasizing the importance of the current study on memorable messages and communication context and the adoption of protective behavior against SEAs. The following research questions guided the study inquiry:

> **RQ1:** What behavioral change did Saudi Arabian students abroad take to protect themselves from social engineers' attacks?
> **RQ2:** What forms of communication prompted Saudi Arabian students abroad to take secure behavior to protect themselves from SEA?
> **RQ3:** In what ways did a key message (e.g., cultural, religious, content, sources) influence Saudi students to take protective behavior against fraud in unfamiliar environments?
> **RQ4:** In what ways are memorable messages and taking secure behaviors linked among Saudi students abroad?

Interpretation of the Findings

A total of 72 Saudi students currently enrolled in Western universities completed the

open-ended online survey regarding their fraud-related memorable stories, interactions, and messages influencing their concerns and protective behavior to avoid fraud threats. These participants shared 404 fraud-related stories and messages; these were inductively analyzed using qualitative content analysis technique to identify memorable and influential communication forms that led participants to engage in more secure behaviors to protect their personal information in less familiar interactions. The findings identified two communication themes that enhanced the memorability and impact of fraud-related incidents. One theme emerged as predominant across participants, while the second was less commonly observed in the data. Theme one: the interactivity in fraud awareness was found to enhance the memorability of fraud-related stories and the adoption of secure behavior. Further, the theme revealed participants' internal emotional aspects and behavioral responses toward the fraud threat, encouraging them to be more secure in protecting their information. On the other hand, theme two was the one-way communication, which participants received fraud-related messages from authorities, media, and academic sources, did not appear to enhance the memorability on their own. The following sections discuss each theme along with the associated subthemes in more detail, considering the findings in relation to existing literature on protective behavior change and memorable messages.

Theme One: Interactivity in Fraud Awareness

A key theme from participants' responses reflected that the interactive element is likely to enhance the memorability and impact of fraud-related stories. This theme arises from participants' interpersonal communication, featuring personal stories and interactions with scammers. The second subtheme emphasizes interactive elements from conversations with close others, where they encountered fraud-related stories alongside family and friends. The third

subtheme addresses intrapersonal communication, revealing emotions like fear and distrust, and behaviors such as hanging up or blocking suspicious links and calls. These Interactions, whether self-directed or with others, were present in 308 of the 404 incidents. Several participants experienced overlapping interactions, with some involved in a single communication event and others participating in multiple events. This finding suggests that fraud-related interactions appeared to influence participants' concern about the risk associated with fraud and encourage secure behavior to prevent repeating their fraud experiences or avoid others' fraud experiences. This is consistent with findings from previous studies, which suggest that the most memorable and influential messages are often tied to personal, relevant, social contexts and emotionally impactful experiences (Horstman et al., 2023; Kaufmann et al., 2021; Knapp et al., 1981; Smith et al., 2009; 2010).

Furthermore, the finding suggests that memorable messages were not strictly tied to the format in which social engineering threats were conveyed but were instead shaped by personal relationships and interactions. This finding adds to the existing research on memorable messages and behavioral change to include that messages related to fraud threats may effectively influence secure behavior when they emerge through interaction-based events and social engagement (Anderson et al., 2020; Lucas & Buzzanell, 2012; Kaufmann et al., 2021). Additionally, both direct experiences with scammers and discussions with close others who were fraud victims appeared to influence participants' concerns about fraud and the decision to adopt practices. These interactions contributed to participants reflecting their internal emotional and behavioral responses to avoid fraud attacks. This observation appeared in responses of participants who expressed emotional reactions, such as skepticism and distrust, and behavioral responses, including avoiding over-the-phone transactions and reporting scams to authorities, especially

among participants who interacted personally with scammers and/or close other fraud victims (see Table 11). Accordingly, this confirms what the study suggested: that the interaction events, including conversations with close others, where participants were exposed to fraud-related stories, observing fraud-related consequences within their social environments, and direct interaction with scammers, appeared to influence participants' concern about fraud (emotional reactions) and reinforce the importance of protective measures (behavior responses).

Table 11

Intrapersonal communication and Associated communication Context

Memorable Messages	Interaction events		One-way Communication	**Total Mentions	***%
	Social Exposure[1]	Personal Exposure[2]	Institutional Communication		
***Vigilance Against Fraud**	16	16	1	33	31.42
Avoidance Strategies	14	21	1	36	34.28
Culturally Inspired Wisdom	5	4	-	9	8.57
Institutional Communication	11	11	3	25	23.80
Other' Negative Experiences with Fraud	1	1	-	2	1.90
				F= 105	

Note. The total number of answers included was 118, based on responses to memorable messages (96) and responses within the vigilance against fraud (22). The analyses of responses with communication events resulted in 105 entries, as some participants engaged in multiple interactions and institutional messages. [1] Interpersonal communication: other's fraud stories, [2] Participants' stories with fraud. *This category reflects participants' emotional and behavioral reactions against fraud. **The total number of times each category was associated with an interaction. ***% represents the percentage of total communication context.

Table 11 presents the distribution of memorable messages influencing secure behavior change and responses reflecting participants' vigilance against fraud across the associated communication context. Based on this data, participants appeared to not only recall fraud-related incidents primarily in which they interacted with victims and/or scammers, but also associated

with recalling memorable messages that influenced the decision to adopt secure behavior against fraud attacks. To illustrate, participants' vigilance against fraud and avoidance strategies were among the most frequently referenced categories, 31.42% and 34.28%, respectively. Following that, institutional messages, at 23.80%, are the dominant source of memorable messages from combined exposure to interactive events and institutional messages. However, only a small portion of the reported memorable messages, 3 out of 25, originated solely from institutional communication sources such as authorities and media. One aspect of the importance of the study lies in shedding light on the fact social interaction with close others and/or scammers appeared to not only make participants able to recall fraud-related memorable messages but also to develop protective attitudes (intrapersonal communication) observed through their vigilance against fraud, their awareness of avoidance strategies to prevent potential attacks, and their sense of responsibility to protect their confidential information (see Table 3).

Furthermore, this process of internal reflection seemed to primarily occur among participants who either had personal interactions, experienced fraud attacks, encountered suspicious interactions, or were exposed to others' fraud-related stories. This suggests that participants were more likely to recall fraud-related messages when they engaged in social interactions, personal experiences, or a combination of social interactions and exposure to institutional messages. These findings highlight the role of interactive elements in reinforcing the memorability of fraud-related messages and influencing the concerns about fraud and the adoption of protective behaviors, indicating a connection between interactive communication and the implementation of secure practices against fraud attempts.

Since participants' memorable messages appeared to be shaped by their social interactions, those with personal and emotional connections to fraud victims were more likely to

exercise caution when navigating similar risk settings. One participant mentioned, "*My cousin recently had lost all of the money in her account due to a bank impersonator.*" This story of close others not only made this participant moderately concerned about the fraud risk but also made her recall the message "*Trust no one for confidential information over a phone call*" as a memorable strategy against fraud. Furthermore, the participants' interactions with scammers made fraud-related messages more memorable. This was evident when participants confronted risk directly; those experiences were impactful and encouraged more secure behaviors among individuals who had faced harmful fraud attacks. For example, one participant stated that his personal experiences with fraud not only made him concerned about filing as a fraud victim but also taught him that "*the less you share, the more safe you are"* as a memorable strategy against scammers.

Similarly, another participant who suffered harmful fraud attacks and also observed close others' fraud stories said, "*Always question people and companies' intentions when asking for your personal information*" as a memorable advice to securely navigate the websites and social media platforms where the participant and her father got scammed. Non-harmful fraud experiences were also memorable and influential in adopting secure actions; these were where participants engaged in suspicious interactions with scammers. For example, a participant who reported concerns of potential fraud threats due to the "*Repetitive unknown emails and texts*" adopted strategies like "*Always check email address before responding*" as a memorable strategy to avoid potential fraud attacks. The following subsections focus on interpreting and synthesizing the findings of related subthemes that contributed to the development of interactive in fraud awareness theme.

Subtheme One: Interpersonal Communication (own)

Out of the 404 incidents, 120 fraud-related stories were about participants' direct interactions with scammers. These stories were shared by 52 participants, some of whom recounted multiple fraud-related incidents. These stories occurred when participants either engaged in suspicious interactions or experienced harmful fraud attacks through various channels, such as email, phone calls, or text messages. These findings suggested that interaction with scammers emerged as a notable communication event in recalling stories and reinforcing the adoption of secure practices. Since not all fraud interactions result in financial losses, the perceived risk of loss can still emotionally impact participants, influencing their secure behavior. One participant who experienced a not-harmful incident said, "*It was an attempt to withdraw money from my card."* This participant said, "*My friend & I were always careful to the point we were surprised that we were actually tricked*!" Another participant who experienced a perceived risk of loss expressed, "*I get a lot of job offers that's obviously a scam while I recognize it now I worried it will be developed to a point where it can deceive me*".

These feelings of the perceived risk of loss are essentially a negative outcome of the prevalence of sophisticated fraud attempts targeting individuals; however, these feelings of discomfort associated with the potential of becoming fraud victims and losing something valuable were often essential to adopting more secure practices (Hazari et al., 2008; Parsons et al., 2014; Tschakert & Ngamsuriyaroj, 2019). Expanding on studies about the role of emotions, such as the perceived risk of loss influencing participants' concerns about fraud, Loewenstein et al. (2001) revealed that risk-related feelings interact with individuals' cognitive evaluations, such as desired outcomes, ultimately shaping decisions and behavior changes. This aligns with the findings of the current study, in which mere interaction with scammers, such as suspicious interactions or non-harmful experiences, has led participants to recognize the threats associated

with fraud and motivated them to adopt secure behavior. These findings indicate that the feelings of concern that participants reported motivated risk-averse behavior. Given that several participants engaged in interactions with scammers, several studies have found that past experience, whether negative or positive, shapes the attitude and motivation to change behavior (Albarracin & Wyer 2000; Sidor & Dubin 2025). The influence of experience was found to mainly impact the individual's cognition and recognition of the consequences of a behavior, which directly affects attitudes and the ultimate behavioral decision (Albarracin & Wyer 2000). In the current study, participants who had a harmful experience with fraud attacks or engaged in suspicious interactions were likelier to feel the threat targeting their information and financial matters. This can highlight that participants' awareness of the consequences of falling victim to fraud and losing something valuable can influence the likelihood of forming a protective attitude toward safer behavior. This was discussed in the Theory of Reasoned Action, which suggests that individuals' intentions and decisions are influenced by their attitudes toward a behavior and their expectations of positive outcomes. Consequently, individuals believe that a specific action will result in favorable results; this belief directs their behavior toward achieving those outcomes (Fishbein & Ajzen, 1975).

Therefore, the current study contributes to understanding the role of personal experience in recalling messages that shaped behavioral responses. This finding aligns with a study by Haselhuhn et al. (2012), who challenged the idea that learning new information is simply about acquiring facts, suggesting instead that experiential learning plays a crucial role in shaping knowledge and influencing decision-making. Their conclusion was based on observing behavioral changes in individuals who had experienced paying a late fee during a rental period (Haselhuhn et al., 2012). In the current study, participants' experiences with scammers appeared

to be one of the memorable interactions—both harmful and non-harmful—that influenced their protective attitudes through intrapersonal communication. These findings align with previous studies emphasizing that fraud risk cannot be fully mitigated until all users develop a sense of caution and adopt safer practices (Sipayung et al., 2022; Talib & Rusly, 2015; Yuniarti & Ariandi, 2017; Zahari et al., 2019). Overall, according to the theme and past supporting literature, past experiences with scammers, even those that resulted in no losses, were notably compelling in leading participants to be more aware of the suspicious fraud strategies and demonstrating more secure practices that were seen through recalling several avoidance strategies, authority warning, and cultural messages. The current study findings can be a reference for future studies to the fact that personal interaction (past experience) with scammers could be one form of communication that effectively leads individuals to be more fearful and suspicious (emotional reaction) in protecting confidential information (behavioral response).

Subtheme Two: Interpersonal Communication (close others)

Based on the data, 68 fraud-related stories were shared through family, friends, and peers. These stories were reported by 40 participants, with some participants recounting multiple fraud-related stories. Existing studies on personal connections and conversations contribute to individuals' perceived risk and attitudes toward fraud (Albrechtsen & Hovden, 2010; Andrews and Boyle, 2008; Pervaiz et al., 2019). Building on these, the current study reveals that exposure to others' harmful fraud stories helped participants develop protective attitudes against SEAs, highlighting the connection between these interactions, fraud recognition, and adopting safe practices. This suggests that a personal and emotional connection with other victims was vital in raising awareness of fraud risk by making the threat seem closer and more tangible. This indicates that interactions with others motivated participants to learn from other's experiences

and adopt safe practices to prevent encountering similar risky situations. This is also consistent with Bandura's Social Cognitive theory, which suggests that individuals can learn and be motivated to adopt behaviors through vicarious experiences. Furthermore, the current findings align with prior studies revealing that exposure to others' negative experiences about fraud risk, particularly with family and peers, can motivate individuals to adopt secure behavior (Rader et al., 2012; Redmiles et al., 2016). For example, participants who shared their peers' negative experiences with fraud were able to recall messages demonstrating their emotional and behavioral responses to avoid potential SEAs. According to the findings and past supporting literature, storytelling from family and friends has always been a compelling factor that contributed to behavior change and attitudes toward an issue. The current study supports the significant role of storytelling and conversations with close other as a source of fraud-related information, motivating individuals to navigate less familiar interactions securely (Albrechtsen and Hovden 2010; Hinyard & Kreuter 2007; Ogata Jones et al. 2006). This study is expected to be an addition to the role of conversation on individuals' protective attitudes against SEAs.

In the context of Saudi Arabia, the current findings revealed that participants appeared to be able to share and exchange stories about fraud within their social interactions. These findings challenge the common ideas of social stigma associated with fraud victims in Saudi Arabia, in which social expectations (social pressure) and Islamic principles deeply shape cultural norms in Saudi Arabia, especially concerning financial matters (Ahmed, 2021; Mathkur, 2019; Siddiqi, 2004). In Saudi culture, individuals are expected to be financially responsible, and falling victim to scams can be perceived as a personal failure, often carrying that social stigma. This challenge was based on responses about sharing fraud-related experiences within their social circles and personal stories. It was also identified as one of the secure practices reported by participants,

such as social vigilance and communication, in which participants reported talking with close others about any fraud-related topic, as shown in Table 3. However, it is also possible that participants who reported concerns about fraud and reported practices secure actions to protect themselves (*n*= 153) but have not disclosed their sources of these responses may indicate an underlying stigma (see Table 2). Therefore, this study initiates a critical discussion on the social stigma associated with fraud victims, an area for future research to further shed light on how social perceptions (fraud stigma) influence individuals' vigilance and willingness to share fraud incidents. In the current study, given that the participants did not explicitly reference cultural stigma as a reason for sharing or holding fraud-related information, future studies could explore how participants framed their fraud experiences, indicating ways to minimize their responsibility for such incidents as shifting blame or emphasizing external causes.

Subtheme Three: Intrapersonal Communication (Protective Attitude)

Out of the 404, 120 responses demonstrated emotional reactions, such as distrust, fear, and concern about the SEA risk, and behavioral responses to overcome that emotion, such as avoidance strategies and reporting attacks. Intrapersonal communication as a subtheme in the current study is reflected in participants sharing their internal thoughts and emotions about fraud, and these were seen through responses including their vigilance against fraud, their awareness of avoidance strategies to prevent potential attacks, and their sense of responsibility to protect their confidential information (cultural-based messages). One key aspect highlighted in the current study is that participants' reflections align with the concept of protective attitudes, which develop primarily through their interaction with fraud-related, either by observing others' experiences or through their own encounters with fraud. In psychology and health research, a protective attitude refers to an individual's mental state that motivates them to protect themselves against perceived

threats (Wilson, 2021). This mindset often motivates individuals to either take preventive actions to reduce vulnerability, such as avoiding phone or online transactions—or adopt protective behaviors to mitigate potential harm, such as checking website links before clicking them. While protective behavior involves tangible action taken to prevent threats, attitudes, as defined in psychology, represent an individual's evaluation of whether positive or negative of certain ideas or behavior (Lopez et al., 2018; Slovic, 1978). These findings suggest that participants' protective attitudes—feeling concerned about fraud and their behavioral responses—were associated with memorable interactions, reinforcing the importance of both personal and vicarious experiences in shaping secure behavior against SEAs.

Furthermore, this protective attitude toward avoiding a threat aligns with the Protection Motivation Theory (PMT), which suggests that individuals assess their vulnerability to a threat and their ability to cope with it (Rogers, 1975). According to PMT, individuals who believe in the effectiveness of protective behavior and have confidence in their ability to perform it (self-efficacy) are more likely to take protective action. Conversely, individuals who perceive a threat as severe and believe they are highly vulnerable to it may experience heightened fear, which can either motivate them to take preventive actions or lead to avoidance of a threat source (Bandura, 1997; Maddux and Rogers, 1983; Rogers, 1975). While both cognitive appraisals contribute to behavior change, individuals' self-efficacy in avoiding a threat significantly influences their intention to adopt the recommended behavior (Maddux & Rogers,1983). In the same context, the Health Belief Model (HBM) further expands this framework by incorporating perceived benefits, barriers, and cures to action as key determinants of behavior change in response to a threat (Becker & Rosenstock, 1987; Rosenstock, 1974). Consistent with previous studies, the findings of this study indicate that participants evaluated potential threats emotionally, considering their

awareness of scammers exploiting advanced technology as one participant shared "*AI technology made some videos or messages seem very believable*" (perceived susceptibility) and scammers' persuasive tactics to manipulate potential victims as one participant shared " *money was stolen through unintentional disclosure of their account info which resulted in loss of money.*" (perceived severity). Furthermore, participants' adoption of secure behaviors appeared to be influenced by (perceived benefits), such as adopting multiple and varied secure practices, and cure to actions, such as hearing others' fraud stories, especially personal ones, along with their encounters with scammers and institutional warnings, all of which played a to influence the perceived fraud risk and the effectiveness of adopting protective measures. In both interaction events (interpersonal interaction with others and with scammers), participants' efficacy and positive attitude toward particular behavior outcomes are among the factors that promote secure behavior against fraud risk. In addition to the role of interactive communication, the current findings support the existing studies in which individuals perceive the risks, perceived benefits, and cures to actions as factors that trigger their intention to take action against SEAs.

In line with previous studies on the relationship between memorable messages and behavior change (Brown & Wingate, 2022; Cooke-Jackson & Rubinsky, 2021; Kuang et al., 2023), memorable interaction events can also foster anticipatory protective attitudes even before individuals face a threat. In SEA interventions, these findings suggest that the influence of messages is not limited to the content of the messages themselves; rather, the interactive context in which they were conveyed can also shape individuals' emotions and behaviors over time. The current study suggests that the communication process, where participants exchange stories through interpersonal interactions or firsthand engagement with fraud, played a notable role in evoking participants' emotional reactions to SEA risks and precautionary behavior to avoid

potential risk. Ultimately, fraud-related memorable messages and interactions influence participants by providing expected risks, decision premises, and preferred attitudes. The current study can further illustrate how protective attitudes toward fraud risk emerge through social interaction and past experiences, creating lasting impacts on individuals' memories.

One aspect that should be highlighted in the study is that 10 participants reported no concern about the fraud risk due to their confidence in recognizing fraud attempts. Although these participants have reported firsthand encounters with harmful fraud attacks, engaged in suspicious interactions with scammers, and shared fraud-related incidents through others. Out of 10, 4 participants provided memorable messages influencing their decisions to protect against SEAs. In this regard, considering Bandura's concept of self-efficacy, it appears that participants' confidence in their ability to avoid fraud attacks reduced their level of concern about potential threats. This idea was based on the fact that some of these participants shared the story behind their reaching confidence and protective behavior. For example, one participant shared that "*خبرتي السابقة للعمل في البنوك اكتسبت المهاراة التي تساعدني على ذلك*." (My previous experience working in banks has given me the skills to do this.) On the other hand, these findings can also align with past studies suggesting that, despite individuals' confidence in their anti-threat awareness and protective measures, notable gaps in their knowledge and understanding persist (AlSulaimi, 2022; Furnell et al., 2007). These gaps were also found among novice users, underscoring that even expert users are at a high risk of falling victim to fraudulent tactics (Pervaiz et al., 2019; Visa, 2023).

These gaps are particularly evident among participants who have not experienced an emotionally impactful reaction from their direct encounter with fraud (not concerned about fraud risk), making them appear less vigilant toward potential future fraud. Based on previous studies,

participants who expressed a low perceived risk of threats are more likely to be challenged to pay attention to threat-related messages because they do not perceive the issue as relevant to them (Rogers, 1983; Witte, 1992). These studies explain how individuals respond to threat-related messages, emphasizing that those who perceive low-risk threats and possess self-efficacy are less likely to pay attention to these messages or engage in protective behaviors. Consequently, this communication challenge in avoiding anti-fraud awareness among participants who feel invulnerable makes them less likely to adopt appropriate secure actions regarding how scammers enhance their strategies by leveraging advanced technology and uncertain situations (Ma & McKinnon, 2021; Steinmetz et al., 2020). Furthermore, the findings build on studies exploring secure behavior adoption, such as Davinson and Sillence's (2014) work, which explains why some individuals perceived the fraud risk as low and showed little concern for preventive measures. These factors include a lack of responsibility and uncertainty about protective actions. Additionally, the current study extends this, suggesting that several aspects can challenge participants to evaluate their fraud stories and recall memorable messages, including the significance of past encounters and the challenge of remembering past events. Lastly, these findings challenge the notion that individuals have a low perceived threat level of scams, so they do not adopt protective measures (Dodge et al., 2012; Langenderfer & Shimp, 2001). The current findings may reference that, despite perceiving the risk as low, participants still reported engaging in secure behaviors against SEAs.

Theme Two: One-Way Communication

Out of the 404 incidents, 37 responses were about receiving fraud-related warnings through communication tools targeting public audiences; according to the 17 participants, these sources include authority warnings, academic instruction, news media, and social media posts.

The current study aligns with the argued findings of the effectiveness of mass media messages in behavior change (Smith et al., 2001; Snyder, 2007; Wakefield et al., 2010). Based on the responses, this study suggested that one role of the mass media messages was to inform audiences about the risk of their information being targeted by malicious attackers. However, in line with the past studies on media-based and memorable messages, the current findings demonstrated that participants could recall being exposed to warning messages about the risk of fraud. Still, participants did not provide detailed information on media stories other than mere exposure (Cialdini, 2009; Hinyard & Kreuter, 2007; Redmiles et al., 2016). Further, this aligns with the study by Davinson and Sillence (2010), who found no impact of the training program and self-responsibility on encouraging users to adopt secure behavior.

Furthermore, in the context of combating social engineering that is known to be continuously refined in attacks leveraging digital technology and uncertain situations, institutional messages can fall short of addressing the various strategies the scammers use to deceive potential victims (Hadnagy, 2010; Steinmetz et al., 2020; Talib & Rusly, 2015). The limitation in addressing the complex SEA schemes was evident in the responses, which indicated that the one-way messages, including mass media messages, often focus narrowly on not sharing passwords and verification codes with others. Nevertheless, this achievement of warning people not to share or to be aware of the potential attacks highlighted that mass media messages appeared important for reducing the risk of sharing verification codes and passwords with others. Still, based on the responses and several news articles, SEA risk is nowadays becoming more complex, and individuals are more in need to recognize the various sophisticated scams attempts such as sending money to a scammer for counterfeit service or products, requesting payment of a shipment fee scams, fraudulent package release fees, and mimicking official brand sites, etc. (Al-

Dhaban, 2025). Therefore, the current findings highlight that, unlike other risk behaviors, individuals must not only adopt the recommended protective measures or change others but also be able to recognize the fraud risks. This fraud recognition may motivate them to educate themselves about scammers' various strategies. This aligns with the review on the effectiveness of mass media campaigns to promote behavior change, revealing consistent evidence on achieving behavior change on proximal outcomes, while the distal outcomes were mixed (Den Braver et al., 2022). As presented in Table 11, the relationship between recalling memorable messages and adopting secure behavior was evident among participants already engaged in interactive communication and also had exposure to institutional messages.

These findings align with Ogata Jones et al. (2006), who found that double exposure—through both interpersonal communication and media messages—was effective in encouraging women's breast screening practices. Following previous studies, this means that holding personal relevance and emotional connection with the fraud-related stories heightens fraud concerns and encourages adopting particular strategies against fraud (Davis et al., 2016; Hinyard & Kreuter 2007). Institutional communication, including mass media messages, authority warnings, and academic instruction, can play an essential role in helping individuals recognize the risks associated with SEAs. However, the current study's evidence was more inconsistent regarding the effectiveness of such messages alone than when incorporated with other interactive communication, such as interpersonal discussions with other fraud victims and individuals' direct experiences with scammers.

Summary of the Findings and Interpretation

This study explored the forms of communication, using memorable messages as a framework, that influenced Saudi students abroad to be concerned about the risk associated with

SEAs and to take secure behavior to avoid such risk. The participants revealed that their connection with close other and their direct stories with scammers impacted their fraud concerns, encouraging them to adopt secure behavior against the risk. These interactions with close others and with scammers have resulted in the participants' intrapersonal communication (protective attitudes) reflecting their emotional reactions and behavioral responses to avoid fraud attacks. These reflections demonstrated across the memorable messages that influenced adopting secure behavior, which were provided mainly by participants who engaged in interactive communication. Indeed, the current study found that participants have made notable behavioral changes to protect themselves from social engineering attacks, with most reporting adopting various secure practices. These secure behaviors were categorized to illustrate participants' comprehensive approach against fraud, incorporating both technical and interpersonal strategies. Participants shared general fraud experiences that heightened their concern about potential attacks on their personal information, noting that investigating less familiar interactions abroad has not seemed to impact their fraud concerns.

Furthermore, participants were able to recall several forms of communication, including interpersonal, intrapersonal, and institutional communication, with interactive communication appearing across the responses, patricianly engaging in fraud-related storytelling with close others, and participants' encounters with scammers. The current study suggested that participants have developed several protective attitudes; this was reflected in participants' emotional reactions, such as fear, threat, and distrust, as well as the behavioral response to overcome these emotions, such as avoidance and using responsible behavior. Those participants engaged in interactive communication could share memorable messages that influenced their adopting secure actions, highlighting their behavior responses to fraud concerns (avoidance strategies) and

their self-responsibility to protect themselves against fraud (culturally inspired wisdom), reflecting Saudi culture and Islamic religion as a key message. In recalling fraud-related memorable messages, sources did not appear to shape the memorability of the message. However, few participants reported that media messages, particularly authority warnings, were memorable messages to act more cautiously. Following the findings, the study suggested that interactivity in processing fraud-related information through interaction with others and participants' internal assessments has resulted in participants recalling practical and personal messages driven by their fraud experiences. This indicates that the connection between memorable messages and adopting secure behavior is often established through participants' interactions, active exchange of fraud-related stories with others, and internal evaluations.

Limitations

This qualitative case study aims to explore the fraud-related stories of Saudi students studying abroad in Western countries, examining how different forms of communication, particularly memorable messages, are associated with participants' concerns and adoption of secure behaviors against SEAs in less familiar interactions. Therefore, the study was designed using an open-ended survey data collection approach, which increases the possibility of limitations of the study findings that should be acknowledged (Creswell, 1994; Guba & Lincoln, 1994; Patton, 1987). This study has proven challenging as it involves recalling memorable fraud-related incidents, making participants recollect selective, dramatic, or emotionally impactful incidents or unable to remember them. As such, several conclusions mainly rely on the participants' input, willingness, and desire to share their fraud-related stories. Another limitation during the data collection was that some participants left some responses incomplete or blank, which may be due to their lack of time or motivation to provide detailed responses to qualitative

questions. This could influence the comprehensiveness of the findings. Thus, the conclusions drawn from this study depend heavily on the quality and depth of the participants' input, in which their inability to recall fraud-related experiences or articulate their thoughts effectively may influence the richness of the findings (Geer, 1988; LaDonna et al., 2018). Further, the scope of fraud, scams, and hacking activities is not limited, so the study may not cover or explain all SEA methods (Chen, 2024; Hasham et al., 2019). Thus, the analysis focuses primarily on the SEA activities participants have encountered or shared in which they experience financial losses and information leakage resulted by human-based or technology-based attacks. Further, the criteria for participants' inclusion included Saudi students who enroll in Western countries, whose cultural context may shape their experiences and perspectives and may differ from those of local students or other international students. As such, this limits how applicable the findings and the application of these findings to other cultures or geographic settings. Acknowledging these limitations, future research should consider addressing these limitations by exploring a more diverse sample and employing methods to encourage fuller and more detailed participants' responses.

Future Research Recommendations

This study yields several recommendations. Future researchers can extend the scope of their exploration to investigate other foreign communities living in less familiar interactions where people speak different languages and have unique cultural norms, such as international students, tourists, and immigrants secure behavior against SEAs. This opportunity exists for future studies to replicate and further validate the results in determining whether communication forms contribute to people's risk concern and their adoption of protective behaviors against potential SEAs. Such a study might be valuable because the current research only included Saudi

students abroad in Western countries, in which these countries have several differences in the language, culture, and local system. Another recommendation for future studies is to use a multiple case study design. The current study explores communication forms that contribute to concern about fraud and adopting secure behavior, focusing on Saudi students studying in Western countries, including the US, UK, and Austria, as a case study. It might be valuable to employ a multiple case study to allow the researcher to explore the communication forms across multiple cases, such as local students and students abroad. Such a study would allow the researcher to identify the differences and similarities of forms of communication and memorable messages across the different cases.

Furthermore, the current study included Saudi students abroad who are age 18 and above as the sample. As such, the findings of this study do not represent a specific age group but focus on a sample of students abroad navigating less familiar interactions than in their home country. Having a wide range of ages from 18 to 64 among participants may introduce differences in their experiences, knowledge, and risk perception, influencing their emotional reactions to risks and adoption of secure practices. Future researchers can explore the issue by focusing on particular age groups, such as the traditional age of college students over 18 and under 25, as the sample. Given the limitations presented in the study, a future researcher should consider expanding the sample size, either by including a broader range of countries where Saudi students studied or by increasing the overall population size. Furthermore, the current findings concluded that two-way or interactive communication appeared to influence participants' concern about fraud and the adoption of secure behavior compared to one-way communication, such as mass media messages, academic instruction, and authority warnings. Thus, a future researcher can consider an extensive literature review of the impact of various communication strategies, including

published studies on social media anti-fraud campaigns and/or published studies on traditional media strategies' role in SEA prevention initiatives. These reviews can summarize the evidence of the effectiveness of behavior change or determinants fraud-related recommendations to successfully raise public concern about the SEA risk and the adoption of secure behavior.

Furthermore, an opportunity exists for future studies to replicate and further validate the findings, in which we found that interpersonal communication (with close other and personal experiences) has participants to reflect on their emotional reaction and produce behavior responses. Further studies following the memorable messages framework to explore factors influencing secure behavior change can also extend the findings across other foreign or local participants to validate the results. The current findings have resulted in memorable messages reflecting participants' internal thoughts and evaluation, which influenced the adoption of secure behavior against SEAs, focusing on avoidance strategies and self-responsibility.

The participant's memorable messages findings also highlighted the role of cultural and religious values in fraud prevention, which were reflected through the culturally inspired wisdom shared by Saudi students who participated in the study abroad. Thus, one more recommendation for future studies is to investigate fraud-related memorable messages of Saudi students in their home country to link further key messages influencing them to adopt secure behavior. Furthermore, this study suggests that the participants' responses reflected a willingness to share incidents of fraud and harmful experiences related to fraud attacks in their social environments, indicating a need to explore the common notion of the social stigma associated with fraud victims in Saudi Arabia. Thus, future qualitative studies could explore how participants framed their fraud-related stories, indicating ways to minimize their responsibility for such incidents as shifting blame or emphasizing external causes.

Theoretical Implications

The findings of the current study offer several theoretical contributions by emphasizing the connection between participants' memorable messages, their behavioral changes, and the theories of protective behavior and interaction effects discussed earlier. For example, the concept of social learning appeared to reinforce protective behavior, as concern about fraud was influenced after participants heard fraud-related stories from close others, such as family members and friends. This demonstrates the power of vicarious experiences and social modelling in behavior change introduced in Bandura's Social Cognitive Theory, particularly within highly interactive and collectivist cultures like Saudi Arabia. Furthermore, the influence of close others in adopting secure behavior against fraud attacks highlights the significance of normative and subjective beliefs in shaping intentions and actual actions. As participants' memorable messages reflected how Saudi culture and religious values emphasize caution through self-responsibility and moderation in financial matters. This is consistent with the theory of planned behavior (TPB), where others' expectations and perceptions of particular behavior, such as advice from close others and religious teachings, contributed to participants' decisions to adopt secure behaviors.

In addition, participants' vulnerability to the evolving fraud attacks and their behavioral responses to avoid such attacks are observed to be critical motivators, which is consistent with the Protection Motivation Theory's (PMT) predictions. Similarly, the study findings also suggested that participants weighed the seriousness and susceptibility to sophisticated fraud schemes alongside the perceived benefits of taking secure actions, which are related concepts introduced in the Health Belief Model (HBM). Overall, while these findings suggested that factors like social learning, self-efficacy are among the universal aspects of context influencing

the protective behaviors, other factors such as cultural and religious values and close others' emotional narrative communication appear especially important in the Saudi context to directly influence concerns and reinforce secure behaviors.

Practical Implications

Given this study's findings, various forms of communication can potentially drive secure behavior change against SEAs. At all levels, including mass media, organizations, and individuals, adopting secure behavior against SEAs was found to be driven by the participant's emotional reactions such as distrust and suspicions, producing behavior responses to avoid the potential SEA risk (intrapersonal communication). Considering that these findings resulted through participants' interactive communication with others and/or direct experiences with scammers, interpersonal communication may be used to develop better ways to evoke risk-feeling emotions, fostering individuals to find their way to overcome these feelings (Hazari et al., 2008; Parsons et al., 2014; Tschakert & Ngamsuriyaroj, 2019). Students abroad are at high risk of being fraud victims not only because of their vulnerability in dealing with less familiar interactions but also because they are targets of sophisticated scam activities such as job scam offers, visa fraud, and impersonation by fake immigration authorities (G Olivier , 2023; Scown, 2019). Furthermore, international students often experience some difficulties of isolation, social belonging, and anxiety in their adjustment phases in a new environment (Akanwa, 2015; Andrade, 2006).

Therefore, at the academic level, colleges and stakeholders can develop programs to raise students' awareness of the risks targeting them by encouraging them to share or exchange their fraud-related stories with others in their social and school environments. Institutional strategies should consider the role of interpersonal communication in individuals' emotional reactions and

behavior responses (distal outcomes) to adopt secure behavior against SEAs. Concern about SEAs and the adoption of secure practices appeared to be more likely when individuals exchanged fraud-related information and stories with others; therefore, it is essential to combine institutional prevention initiatives with programmers within the community in schools, workplaces, and local markets to discuss the issue in person. Notably, many schools use required online anti-fraud courses for all students, incorporating multimedia features and fraud-related scenarios. However, several studies suggest that such training may be ineffective in changing behavior, as it often fails to engage participants meaningfully or tailor content to their real-world experiences (Ceesay et al.,2018; Davinson and Sillence, 2010; Kumaraguru et al., 2007). Therefore, in classes, students can be encouraged to share their fraud-related stories (optional) as one of the academic instructions to recognize the risk associated with the SEAs in person.

At the media level, mass media campaigns can also incorporate and encourage individual arrangements by focusing on structure and monitoring network platforms, such as creating social media hashtags encouraging individuals to share their fraud-related stories and focusing on engagement elements such as replies, retweets, and likes from the stakeholders. Message designers for anti-SEA initiatives are essential in creating effective messages to raise individuals' recognition of the threat associated with fraud, focusing on coordinating and aligning the messages on the local and national levels. For example, local citizens might be at risk of fraud activities other than those targeting foreign communities. Therefore, tailoring the language use, message content, and channel can make a difference in raising individuals' emotional and behavioral responses against SEAs (Bullee & Junger, 2020; D'Andrea et al., 2022). Further, message designers can leverage the role of interactivity in influencing individuals' concerns about fraud and fostering adopting secure behavior. Thus, this can be achieved by designing

messages that encourage audiences to engage in conversation with one another, reinforcing fraud recognition and producing protective attitudes (emotional reaction and behavior response).

Conclusions

The current exploratory study aimed to explore and determine the forms of communication following the memorable messages framework (Knapp et al., 1981), that contributed to adopting secure behavior against social engineering attacks among Saudi students abroad in Western countries. This research was conducted to contribute to the literature on the role of communication forms and memorable messages in behavior changes and to identify the challenges students abroad face in protecting their personal information with less familiar interactions. With a qualitative study approach, following inductive, exploratory approach, the findings revealed the effective role of interpersonal communication, including interaction with other fraud victims and direct experiences with scammers. One of the practical aspects of the study is the addition of interactive elements in addressing complex issues such as fraud, which resulted in a third form of communication in the current research: intrapersonal communication.

This reflected participants' emotional reactions to the fraud risk, including fear, concern, and distrust, producing behavioral responses to overcome these emotions, such as practicing verification and implementing privacy controls (see Table 4). This indicates the effective role of interactive processes in communicating and exchanging fraud-related information, stories, and encounters, influencing participants' concerns, and encouraging them to adopt secure practices. Institutional communication includes authority warnings, academic instruction, news media, and social media posts, which were presented across the participants' responses as a source warning them of the risk associated with SEAs. However, the presence of institutional exposure was always incorporated with interpersonal interactions with scammers and other victims, such as

family and friends, challenging its role on its own. In general, the open-ended survey results showed more consistency in the interactive communication with other victims and scammers on outcomes (emotional reaction and behavior responses) than one-way communication outcomes (awareness and recall).

Furthermore, memorable messages shared by participants influenced their adoption of secure behaviors against SEAs, highlighted by the role of participants' internal reflections to avoid the threat, particularly recalling avoidance strategies, and emphasized their sense of self-responsibility in protecting themselves. Moreover, this study may serve as a reference for further research, particularly regarding Saudi students abroad' memorable messages that reflected culturally inspired wisdom, such as moderation and responsibility in financial matters. It demonstrates the influence of cultural and religious values as key components in shaping fraud prevention strategies among Saudi students abroad. This study can conclude that trust in others and studying abroad in Western countries did not appear to influence Saudi student participants' concerns or behavioral changes regarding fraud. Instead, participants' responses reflected a sense of distrust and caution that shaped their protective behaviors against potential threats, mostly resulting from fraud-related stories encountered in Saudi Arabia rather than abroad. This suggests that trust did not influence Saudi students' security awareness abroad, and being in a foreign environment did not appear to heighten their fraud concerns.

This research was conducted to contribute toward practical literature to improve prevention initiatives against social engineering attacks. As stated previously, institutions, mass media, and stakeholders should focus more on the interactive and engagement elements, which appeared to influence the concern of Saudi students abroad about SEAs and adopting secure behavior. In the data, there was a limitation in the number of studies available that explored

whether forms of communication can influence individuals' fraud concerns and the adoption of secure behaviors among individuals navigating less familiar interactions, such as international students, immigrants, and tourists. To help bridge this gap, future researchers should focus more on those individuals as they are at high risk of being fraud victims, considering the differences in language, culture norms, and interactions (Atkins & Huang, 2013; Lewin, 2015; Michel & King, 2019).

References

Abdullah, A., Gottschalk, P., Gupta, C. M., Kamaei, M., Stadler, W., & Urzică, A. L. (2024). Perceptions of offender motives, opportunities and willingness for financial crime: an empirical analysis of survey responses in six nations. *Journal of Financial Crime.* https://doi.org/10.1108/JFC-03-2024-0097

Abdul Talib, Y. Y., & Rusly, F. H. (2015). Falling prey for social media shopping frauds: The victims' perspective. *International conference on E-commercial.* https://core.ac.uk/download/pdf/42984237.pdf

Abdullah, A. (2022, October 23). Its history is close to 100 years. Everything you want to know about Saudi educational scholarship and its most important destinations يقترب تاريخه من 100 عام.. كل ما تود معرفته عن الابتعاث التعليمي السعودي وأهم وجهاته. *Aljazeera*. https://www.aljazeera.net/politics/2022/10/23/الابتعاث-التعليمي-السعودي

Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society,* 32(3), 183196. https://doi.org/10.1016/j.techsoc.2010.07.001

Abroms, L. C., & Maibach, E. W. (2008). The effectiveness of mass communication to change public behavior. Annu. *Rev. Public Health*, 29(1), 219-234. https://doi.org/10.1146/annurev.publhealth.29.020907.090824

Abdel Razek, A. N. A. (2012). *An exploration of the case of Saudi students' engagement, success and self-efficacy at a Mid-Western American university* (Doctoral dissertation, University of Akron). http://rave.ohiolink.edu/etdc/view?acc_num=akron1337282450

Abdurahimovna, E. I. (2023). Use of mass media campaigns to change health behaviour. *Ta'lim innovatsiyasi va integratsiyasi, 11*(3), 43-45.

Adkisson, R. V. (2008). Nudge: improving decisions about health, *wealth and happiness.* https://doi.org/10.1016/j.soscij.2008.09.003

Ahmed, S. Z. (2021). An Evaluation of the Anti-Fraud Regime in Saudi Arabia from the Islamic Shariah Perspective. *Universal Journal of Business and Management*, 94-120. https://doi.org/10.31586/ujbm.2021.122

Aivazpour, Z., & Rao, V. S. (2018). Impulsivity and risky cybersecurity behaviors: A replication. *AMCIS 2018 Proceedings. 2.* https://aisel.aisnet.org/amcis2018/Replication/Presentations/2

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior*. Upper Saddle River, NJ: Prentice Hall.

Akanwa, E. E. (2015). International Students in Western Developed Countries: History, Challenges, and Prospects. *Journal of International Students.* https://doi.org/10.32674/jis.v5i3.421

Albrecht, W. S., Albrecht, C. O., Albrecht, C. C., & Zimbelman, M. F. (2012). Fraud Examination. South-Western Cengage Learning. *Mason, OH*.

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security*, *29*(4), 432-445. https://doi.org/10.1016/j.cose.2009.12.005

Albarracin, D., & Wyer Jr, R. S. (2000). The cognitive impact of past behavior: influences on beliefs, attitudes, and future behavioral decisions. *Journal of personality and social psychology*, 79(1), 5. https://doi.org/10.1037/0022-3514.79.1.5

Alghamdi, A. K. H., McGregor, S. L., & El-Hassan, W. S. (2021). Financial literacy, stability, and security as understood by male Saudi university students. *International Journal of Economics and Finance*, 13(7), 7-20. https://doi.org/10.5539/ijef.v13n7p7

Alshebami, A. S., & Aldhyani, T. H. (2022). The interplay of social influence, financial literacy, and saving behaviour among Saudi youth and the moderating effect of self-control. *Sustainability*, 14(14), 8780. https://doi.org/10.3390/su14148780

Al-Ghaith, W. (2015). Understanding social network usage: impact of co-presence, intimacy, and immediacy. *International Journal of Advanced Computer Science and Applications,* 6(8), 99-111. DOI: 10.14569/IJACSA.2015.060813

Alhasan, I. Y. (2023). *Human Factors in Cybersecurity: A Cross-Cultural Study on Trust* (Doctoral dissertation, Purdue University Graduate School). https://doi.org/10.25394/PGS.23271581.v1

Al-Dhaban, M. (2025, January 10). هذا يكفي شركات الاحتيال لا تُلام (Enough: Fraudulent companies are not to blame). *Al Arabiya.* https://www.alarabiya.net/saudi-today/last-news/2025/01/10/هذا-يكفي-شركات-الاحتيال-لا-تُلام

Alyahya, A., & Weir, G. R. (2021, March). Understanding responses to phishing in Saudi Arabia via the theory of planned behaviour. *In 2021 National Computing Colleges Conference (NCCC)* (pp. 1-6). IEEE. https://doi.org/10.1109/NCCC49330.2021.9428823

Almuhammadi, S., & Alsaleh, M. (2017). Information security maturity model for NIST cyber security framework. *Computer Science & Information Technology* (CS & IT), 7(3), 51-62. https://doi.org/10.5121/csit.2017.70305

AlSulaimi, A. M. (2022). Saudi Citizens' Awareness of Cyber Protection Methods. *Ialam*, (31). https://openurl.ebsco.com/EPDB%3Agcd%3A10%3A23016378/detailv2?sid=ebsco%3Aplink%3Ascholar&id=ebsco%3Agcd%3A162684995&crl=c

Almrezeq, N. (2021). Exploratory study to measure awareness of cybercrime in Saudi Arabia. *Turkish Journal of Computer and Mathematics Education (TURCOMAT),* 12(10), 2992-2999. https://turcomat.org/index.php/turkbilmat/article/view/4949

AlArifi, A., Tootell, H., & Hyland, P. (2012). Information security awareness in Saudi Arabia. *CONF-IRM 2012 Proceedings*. 57.https://aisel.aisnet.org/confirm2012/57/

Alanezi, F. (2016). *Perceptions of online fraud and the impact on the countermeasures for the control of online fraud in Saudi Arabian financial institutions* (Doctoral dissertation, Brunel University London). http://bura.brunel.ac.uk/handle/2438/12003

Al-Jaid, A. (2024, June 9). Saudi Digital Currency Law قانون العملات الرقمية السعودي. *Watanksa*. https://www.alwatan.com.sa/article/1148294

Alsaif, M. (2014). *Factors affecting citizens' adoption of e-government moderated by socio-cultural values in Saudi Arabia* (Doctoral dissertation, University of Birmingham). http://etheses.bham.ac.uk/id/eprint/4851

Alanazi, M., Freeman, M., & Tootell, H. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. *Computers in Human Behavior*, *136*, 107376. https://doi.org/10.1016/j.chb.2022.107376

Alotaibi, M., Furnell, S., & Clarke, N. (2016, December). Information security policies: A review of challenges and influencing factors. In *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 352-358). IEEE 10.1109/ICITST.2016.7856729

Alston, W. P. (1969). Feelings. *Philosophical Review, 78*(1), 3–34. https://doi.org/10.2307/2183809

Alraddadi, A. H. (2015). The changing socio-political attitudes of Saudi students studying overseas. *Gulf Policies*.

Alsanea, F. A. (2023). Digital technology and its impact on the social change of the Saudi family. *Network Intelligence Studies*, *11*(21), 41-49. https://seaopenresearch.eu/Journals/articles/NIS_21_5.pdf

Alqasa, K. M., Mohd Isa, F., Othman, S. N., & Zolait, A. H. S. (2014). The impact of students' attitude and subjective norm on the behavioral intention to use services of banking system. *International journal of business information systems*, *15*(1), 105-122. https://doi.org/10.1504/IJBIS.2014.057967

Al-Hamzah, M. (2022, March 17). الابتعاث.. والمنافسة العالمية [Scholarship and global competition]. *Al Arabiya*. https://www.alarabiya.net/saudi-today/views/2022/03/17/الابتعاث-والمنافسة-العالمية

Alsanea, F. B. (2023). Gender Environment Adjustment of Saudi Arabian Students in the United States of America. *Information Sciences Letters:* 12 (5). https://digitalcommons.aaru.edu.jo/isl/vol12/iss5/39

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS quarterly*, 613-643. https://doi.org/10.2307/25750694

Andrade, M. S. (2006). International students in English-speaking universities: Adjustment factors. *Journal of Research in International education, 5*(2), 131-154. https://doi.org/10.1177/1475240906065589

Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon,* 7(1). https://doi.org/10.1016/j.heliyon.2021.e06016

Anderson, J., Britt, R. K., Britt, B. C., Harming, S., & Fahrenwald, N. (2020). Native Americans' memorable conversations about living kidney donation and transplant. *Qualitative health research*, 30(5), 679 692. https://doi.org/10.1177/1049732319882672

Andrews, L., & Boyle, M. V. (2008). Consumers' accounts of perceived risk online and the influence of communication sources. *Qualitative Market Research: An International Journal*, *11*(1), 59-75. DOI https://doi.org10.1108/13522750810845559

Atkins, B., & Huang, W. (2013). A study of social engineering in online frauds. Open Journal of Social Sciences, 1(03), 23. https://www.scirp.org/html/36435.html

Australia Parliament House of Representatives Standing Committee on Communications (2010), "Hackers, fraudsters and botnets: tackling the problem of cybercrime, the report of the inquiry into cybercrime/house of representatives, standing committee on communications", https://trove.nla.gov.au/work/37494558

Azungah, T. (2018). Qualitative research: deductive and inductive approaches to data analysis. *Qualitative research journal,* 18(4), 383-400. https://doi.org/10.1108/QRJ-D-18-00035

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behavior? *International Conference on Cyber Security for Sustainable Society, 2015. arXiv preprint arXiv*:1901.02672. https://doi.org/10.48550/arXiv.1901.02672

Baker, H. K., Purda-Heeler, L., & Saadi, S. (Eds.). (2020). Corporate fraud exposed: A comprehensive and holistic approach. *Emerald Publishing Limited.* https://doi.org/10.1108/978-1-78973-417-120201036

Baklashova, T. A., & Kazakov, A. V. (2016). Challenges of International Students' Adjustment to a Higher Education Institution. *International Journal of Environmental and Science Education*, *11*(8), 1821-1832. doi:10.12973/ijese.2016.557a

Bandura, A. (1997). Self-efficacy: *The exercise of control*. Macmillan. http://happyheartfamilies.citymax.com/f/Self_Efficacy.pdf

Bandura, A. (1986). Social foundations of thought and action. *Englewood Cliffs, NJ*, *1986*(23-28), 2.

Barge, J. K., & Schlueter, D. W. (2004). Memorable messages and newcomer socialization. *Western Journal of Communication (includes Communication Reports)*, *68*(3), 233-256. https://doi.org/10.1080/10570310409374800

Barge, J. K., & Craig, R. T. (2009). Practical theory in applied communication scholarship. *In Routledge handbook of applied communication research* (pp. 55-78). Routledge. https://doi.org/10.4324/9780203871645

Baror, S. O., & Venter, H. (2019). A taxonomy for cybercrime attack in the public cloud. In *International conference on cyber warfare and security* (p. 505). *Academic Conferences International Limited.* https://www.researchgate.net/publication/335927227

Bassey, E. B. (2024). *Social Media and Community College International Student Engagement at a Mid-Atlantic Community College* (Doctoral dissertation, Morgan State University). http://www.proquest.com/en-US/products/dissertations/individuals.shtml.

Becker, M. H., & Rosenstock, I. M. (1987). Comparing social learning theory and the health belief model. *Advances in health education and promotion*, 2, 245-249.

Berger, C. R. (1991). Communication theories and other curios. Communications Monographs, 58(1), 101-113. https://doi.org/10.1080/03637759109376216

Berger, C. R. (2014). Interpersonal communication. In *An Integrated Approach to Communication Theory and Research*(pp. 274-293). Routledge. https://doi.org/10.4324/9780203887011

Berger, C. R., & Calabrese, R. J. (1974). Some explorations in initial interaction and beyond: Toward a developmental theory of interpersonal communication. *Human communication research*, *1*(2), 99-112. https://doi.org/10.1111/j.1468-2958.1975.tb00258.x

Bingham, T., & Conner, M. (2010). *The new social learning: A guide to transforming organizations through social media*. Berrett-Koehler Publishers.

Bisel, R. S., & Adame, E. A. (2017). Post-positivist/functionalist approaches. *The international encyclopedia of organizational communication*, 1-22. https://doi.org/10.1002/9781118955567.wbieoc168

Bleiman, R., & Rege, A. (2020, March). An examination in social engineering: The susceptibility of disclosing private security information in college students. In *Proc. 15th Int. Conf. Cyber Warfare Secur.(ICCWS)* (pp. 47-56). http://dx.doi.org/10.34944/dspace/365

Blythe, J. M., & Coventry, L. (2018). Costly but effective: Comparing the factors that influence employee anti-malware behaviours. *Computers in Human Behavior*, 87, 87-97. https://doi.org/10.1016/j.chb.2018.05.023

Bonini, S., & Boraschi-Diaz, D. (2012). The causes and financial consequences of corporate frauds. In *Entrepreneurship, finance, governance and ethics* (pp. 295-314). Dordrecht: Springer Netherlands. https://doi.org/10.1007/978-94-007-3867-6_13

Bradburn, N. M., Rips, L. J., & Shevell, S. K. (1987). Answering autobiographical questions: The impact of memory and inference on surveys. *Science*, *236*(4798), 157-161. DOI: 10.1126/science.3563494

Bringer, J. D., Johnston, L. H., & Brackenridge, C. H. (2006). Using computer-assisted qualitative data analysis software to develop a grounded theory project. *Field methods*, *18*(3), 245-266. https://doi.org/10.1177/1525822X06287602

Brody, R. G., Mulig, E., & Kimball, V. (2007). Phishing, pharming, and identity theft. *Academy of Accounting & Financial Studies Journal*, *11*(3). https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=c3f9bedf86614a9ca7cf18197bfbb978f56e6e56

Brown, N. R., & La'Marcus, T. W. (2024). The influence of memorable message receipt on dietary and exercise behavior among self-identified Black women. *In Emergent Health Communication Scholarship from and about African American, Latino/a/x, and American Indian/Alaskan Native Peoples* (pp. 101-110). Routledge. https://doi.org/10.1080/10410236.2021.1962587

Brush, H. M. (2014, June 6). *Phreaking | Telecom Security, History & Techniques*. Encyclopedia Britannica. https://www.britannica.com/topic/phreaking

Brunken, L., Buckmann, A., Hielscher, J., & Sasse, M. A. (2023). {"To} Do This Properly, You Need More {Resources"}: The Hidden Costs of Introducing Simulated Phishing Campaigns. In *32nd USENIX Security Symposium (USENIX Security 23)* (pp. 4105-4122). https://www.usenix.org/system/files/usenixsecurity23-brunken.pdf

Bullee, J.-W. and Junger, M. (2020), "How effective are social engineering interventions? A meta-analysis", *Information and Computer Security,* Vol. 28 No. 5, pp. 801-830. https://doi.org/10.1108/ICS-07-2019-0078

Burkhardt, M. E. (1994). Social interaction effects following a technological change: A longitudinal investigation. *Academy of management journal,* 37(4), 869-898. https://doi.org/10.5465/256603

Button, M., & Cross, C. (2017). Technology and Fraud: The 'Fraudogenic'consequences of the Internet revolution. In *The Routledge Handbook of Technology, crime, and Justice* (pp. 78-95). Routledge.

Caller ID Spoofing. (2024, November 13). Federal Communications Commission. https://www.fcc.gov/spoofing

Caudle, S. L. (1990). Managing Information Resources in State Government. *Public Administration Review*, *50*(5), 515–524. https://doi.org/10.2307/976782

Causadias, J. M. (2020). What is culture? Systems of people, places, and practices. *Applied Developmental Science*, 24(4), 310–322. https://doi.org/10.1080/10888691.2020.1789360

Ceesay, E. N., Myers, K., & Watters, P. A. (2018). Human-centered strategies for cyber-physical systems security. *EAI Endorsed Transactions on Security and Safety*, 4(14). http://dx.doi.org/10.4108/eai.15-5-2018.154773

Chadd, K. (2020, November). *The History Of Cybercrime And Cybersecurity, 1940-2020*. Cybercrime Magazine. https://cybersecurityventures.com/the-history-of-cybercrime-and-cybersecurity-1940-2020/

Champion, V. L., & Skinner, C. S. (2008). The health belief model. Health behavior and health education: *Theory, research, and practice*, 4, 45-65.

Chargo, M. A. (2018). You've been hacked: How to better incentivize corporations to protect consumers' data. *Transactions: Tenn. J. Bus. L.*, *20*, 115. https://ir.law.utk.edu/cgi/viewcontent.cgi?article=1452&context=transactions

Charmaz, K. (2000). Grounded theory: Objectivist and constructivist methods. *Handbook of qualitative research*, *2*(1), 509-535. https://qualquant.org/wp-content/uploads/text/Charmaz%202000.pdf

Charmaz, K. (2006). *Constructing grounded theory: A practical guide through qualitative analysis*. Sage.

Chen, J. (2024, June 3). Fraud: Definition, Types, and Consequences of Fraudulent Behavior. *Investopedia*. https://www.investopedia.com/terms/f/fraud.asp

Cheshire, C., Antin, J., Cook, K. S., & Churchill, E. (2010). General and familiar trust in websites. *Knowledge, Technology & Policy*, 23, 311-331.

Choudaha, R., & Schulmann, P. (2014). Bridging the gap: Recruitment and retention to improve student experiences. Washington, DC: NAFSA: *Association of International Educators.*

Chugh, B., & Narang, L. (2023) Are Fraud-awareness Campaigns Effective? https://dvararesearch.com/wp-content/uploads/2023/12/Are-Fraud-awareness-Campaigns-Effective_Policy-Brief.pdf

Cialdini Robert, B. (2007). Influence: The Psychology of Persuasion. *New York: Collins Business*.

Cialdini, R. B. (2009). *Influence: Science and practice* (Vol. 4, pp. 51-96). Boston: Pearson education. https://www.knjizara.com/pdf/136381.pdf

Coffman, J. (2002). Public communication campaign evaluation. *Harvard Family Research Project,* 1-42.

https://www.dors.it/documentazione/testo/200905/Public%20Communication%20Campaign%20Evaluation.pdf

Cohen, L. E., & Felson, M. (1979). Extend access to American Sociological Review. *American Sociological Review*, *44*(4), 588-608. http://faculty.washington.edu/matsueda/courses/587/readings/Cohen%20and%20Felson%201979%20Routine%20Activities.pdf

Coleman, E. G. (2012). Phreaks, hackers, and trolls. *The social media reader*, 99-119. https://doi.org/10.18574/nyu/9780814763025.003.0012

Cooke-Jackson, A., & Rubinsky, V. (2023). Extending the Roots of Memorable Messages: A Comprehensive Review and Forecast of Memorable Message Literature and Theory. *Health Communication*, *38*(12), 2676–2686. https://doi.org/10.1080/10410236.2022.2105620

Cooke-Jackson, A., & Rubinsky, V. (2021). Theory of memorable messages. *Communicating intimate health, 89-98*.

Corbin, J., & Strauss, A. (2015). *Basics of qualitative research: Techniques and procedures for developing grounded theory* (4th ed.). Thousand Oaks, CA: Sage.

Counter-Fraud Framework Saudi Central Bank. (2022). The Saudi Central Bank (SAMA). https://www.sama.gov.sa/enUS/RulesInstructions/CyberSecurity/Counter_Fraud_Framework.pdf

Cranmer, G. A., & Myers, S. A. (2017). Exploring Division-I student-athletes memorable messages from their anticipatory socialization. *Communication Quarterly*, *65*(2), 125-143. https://doi.org/10.1080/01463373.2016.1197292

Cranor, L. F., & Garfinkel, S. (2005). Security and usability: designing secure systems that people can use. "*O'Reilly Media, Inc."* http://hdl.handle.net/10563/52229

Creswell, J.W. (1994), Research Design: Qualitative and Quantitative Approaches, *Sage, Thousand Oaks, CA*.

Creswell, J. W. (2007). Qualitative inquiry and research design: Choosing among five approaches (2nd ed.). Sage Publications, Inc.

Creswell, J. W. (2013). Steps in conducting a scholarly mixed methods study. *DBER Speaker Series.* http://digitalcommons.unl.edu/dberspeakers/48

Creswell, J.W. and Creswell, J.D. (2017), *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, Sage Publications.*

Creswell, J. W., Klassen, A. C., Plano Clark, V. L., & Smith, K. C. (2011). Best practices for mixed methods research in the health sciences. *Bethesda (Maryland): National Institutes of Health*, *2013*, 541-545. https://www.csun.edu/sites/default/files/best_prac_mixed_methods.pdf

Creswell, J. W., & Miller, D. L. (2000). Determining validity in qualitative inquiry. *Theory into practice*, 39(3), 124-130. https://doi.org/10.1207/s15430421tip3903_2

Creswell, J. W., & Poth, C. N. (2016). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches.* United States: SAGE Publications.

Cross, C. (2019). "You're not alone": the use of peer support groups for fraud victims. *Journal of Human Behavior in the Social Environment*, 29(5), 672-691. https://doi.org/10.1080/10911359.2019.1590279

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, 32, 90-101. https://doi.org/10.1016/j.cose.2012.09.010

Davis, L. A., Morgan, S. E., & Mobley, A. R. (2016). The utility of the memorable messages framework as an intermediary evaluation tool for fruit and vegetable consumption in a nutrition education program. *Health Education & Behavior,* 43(3), 321-327. https://doi.org/10.1177/1090198115599987

Day, D. V., & Harrison, M. M. (2007). A multilevel, identity-based approach to leadership development. *Human Resource Management Review*, *17*(4), 360-373. https://doi.org/10.1016/j.hrmr.2007.08.007

Davinson, N., & Sillence, E. (2010). It won't happen to me: Promoting secure behaviour among internet users. *Computers in human behavior*, 26(6), 1739-1747. https://doi.org/10.1016/j.chb.2010.06.023

Davinson, N., & Sillence, E. (2014). Using the health belief model to explore users' perceptions of 'being safe and secure'in the world of technology mediated financial transactions. *International Journal of Human-Computer Studies,* 72(2),154-168. https://doi.org/10.1016/j.ijhcs.2013.10.003

Dalli, K. (2023, June 14). Is that really law enforcement calling you? A new scam may have you thinking it is. *Consumer Affairs*. https://www.consumeraffairs.com/news/is-that-really-law-enforcement-calling-you-a-new-scam-may-have-you-thinking-it-is-061423.html

Davis, E. M. (2014). *Saudi women international students in the United States: A qualitative examination of cultural adjustment*. Ball State University.

D'Andrea, A., Grifoni, P., & Ferri, F. (2022). Discussing the role of ICT in sustainable disaster management. *Sustainability*, 14(12), 7182. https://doi.org/10.3390/su14127182

Denzin, N. K., & Lincoln, Y. S. (Eds.). (2011). *The Sage handbook of qualitative research*. Sage.

Den Braver, N. R., Garcia Bengoechea, E., Messing, S., Kelly, L., Schoonmade, L. J., Volf, K., ... & Lakerveld, J. (2022). The impact of mass-media campaigns on physical activity: a review of reviews through a policy lens. *European Journal of Public Health,* 32(Supplement_4), iv71-iv83. https://doi.org/10.1093/eurpub/ckac085

Digital Fraud . (2023, August 1). Digital government authority. https://dga.gov.sa/sites/default/files/2023-08/Digital%20Fraud%20-%20Research%20Study.pdf

Dillard, J. P., & Shen, L. (Eds.). (2013). *The Sage handbook of persuasion*. Sage.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information systems research*, *17*(1), 61-80. https://doi.org/10.1287/isre.1060.0080

Dodge Jr, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *computers & security,* 26(1), 73-80. https://doi.org/10.1016/j.cose.2006.10.009

Drisko, J. W. (2024). Transferability and Generalization in Qualitative Research. *Research on Social Work Practice*, 10497315241256560. https://doi.org/10.1177/10497315241256560

Drake, C. E., Oliver, J. J., & Koontz, E. J. (2004, July). Anatomy of a Phishing Email. In *CEAS*. http://www.mailfrontier.com/docs/MF_Phish_Anatomy.pdf.10

D'Souza, P. V. (1992). Electronic mail in academic settings: A multipurpose communications tool. Educational Technology, 32(3), 22-25. https://www.jstor.org/stable/44425598

Duran, R. L., Kelly, L., & Keaten, J. A. (2005). College faculty use and perceptions of electronic mail to communicate with students. Communication Quarterly, 53(2), 159-176. https://doi.org/10.1080/01463370500090118

Ellis, J. B., & Smith, S. W. (2004). Memorable messages as guides to self-assessment of behavior: a replication and extension diary study. *Communication Monographs,* 71(1), 97–119. https://doi.org/10.1080/03634520410001691456

Elo, S., & Kyngäs, H. (2008). The qualitative content analysis process. *Journal of advanced nursing,* 62(1), 107-115. https://doi.org/10.1111/j.1365-2648.2007.04569.x

Elnaim, B. M. E. (2013, December). Cyber crime in Kingdom of Saudi Arabia: The threat today and the expected future. In *Information and Knowledge Management* (Vol. 3, No. 12, pp. 14-19).

https://www.researchgate.net/profile/BushraElamin/publication/309040131_Cyber_Crime_in_Kingdom_of_Saudi_Arabia_The_Threat_Today_and_the_Expected_Future/links/57ff2f9508ae6b2da3c89b36/Cyber-Crime-in-Kingdom-of-Saudi-Arabia-The-Threat-Today-and-the-Expected-Future.pdf

Emigh, A. (2007). Phishing attacks: Information flow and chokepoints. *Phishing and countermeasures*, 31-64. In M. Jakobsson & S. Myers (Eds.*), Phishing and countermeasures*. New Jersey: John Wiley and Sons. https://doi.org/10.1002/9780470086100.ch2

Fishbein, M., & Ajzen, I. (1974). Attitudes towards objects as predictors of single and multiple behavioral criteria. *Psychological Review, 81*(1), 5974. https://doi.org/10.1037/h0035872

Fishbein, M., & Ajzen, I. (1975). Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research. Reading, MA: Addison-Wesley.

Frederick, S. (2005). Cognitive reflection and decision making. *Journal of Economic perspectives*, *19*(4), 25-42. DOI: https://10.1257/089533005775196732

Furnell, S. M., Bryant, P., & Phippen, A. D. (2007). Assessing the security perceptions of personal Internet users. *Computers & Security*, *26*(5), 410-417. https://doi.org/10.1016/j.cose.2007.03.001

Gaydos, L. (2023, July 25). Scammers are impersonating law enforcement, and the call you get may convincing, authorities warn. *NBC Boston*. https://www.nbcboston.com/investigations/consumer/scammers-are-impersonating-law-enforcement-and-the-call-you-get-may-convincing-authorities-warn/3096962/

Geer, J. G. (1988). What do open-ended questions measure?. *Public Opinion Quarterly*, *52*(3), 365-367. https://doi.org/10.1086/269113

Getie Mihret, D. (2014). National culture and fraud risk: exploratory evidence. *Journal of Financial Reporting and Accounting*, *12*(2), 161-176. https://doi.org/10.1108/JFRA-10-2012-0049

Gentles, S. J., Charles, C., Ploeg, J., & McKibbon, K. A. (2015). Sampling in qualitative research: Insights from an overview of the methods literature. *The qualitative report*, *20*(11), 1772-1789. https://bpb-us-e1.wpmucdn.com/sites.nova.edu/dist/a/4/files/2016/01/Gentles_Sampling-2016-01-16.ppt.pdf

Gentles, S. J., Charles, C., Ploeg, J., & McKibbon, K. (2015). Sampling in Qualitative Research: Insights from an Overview of the Methods Literature. *The Qualitative Report,* 20(11), 1772-1789. https://doi.org/10.46743/2160-3715/2015.2373

Geertz, C. (2008). Thick description: Toward an interpretive theory of culture. In *The cultural geography reader* (pp. 41-51). Routledge.

Ghauri, P., Grønhaug, K., & Strange, R. (2020). *Research methods in business studies*. Cambridge University Press.

Gibbon, R. J. (2021, July 8). The Kingdom of Saudi Arabia approves new Anti-Financial Fraud and Deceit Law. *The national law review.* https://natlawreview.com/article/kingdom-saudi-arabia-approves-new-anti-financial-fraud-and-deceit-law

Glanz, K., Rimer, B. K., & Viswanath, K. (2008). Theory, research, and practice in health behavior and health education. In K. Glanz, B. K. Rimer, & K. Viswanath (Eds.), *Health behavior and health education: Theory, research, and practice* (4th ed., pp. 23–40). Jossey-Bass.

Glaser, B., & Strauss, A. (2017). *Discovery of grounded theory: Strategies for qualitative research*. Routledge. https://doi.org/10.4324/9780203793206

Glass, G. V. (1976). Primary, secondary, and meta-analysis of research. *Educational researcher*, *5*(10), 3-8. https://doi.org/10.3102/0013189X005010003

Glaser, B. G. (2014). Choosing grounded theory. *The Grounded Theory Review*, *13*(2), 3-19. https://groundedtheoryreview.com/wp-content/uploads/2014/12/CHOOSING-GROUNDED-THEORY-2014.pdf

G, Olivier. (2023, November 8). 4 nasty international student scams to watch out for. *Edvoy.* https://edvoy.com/articles/4-nasty-international-student-scams-to-watch-out-for/

Gomes, C., Berry, M., Alzougool, B., & Chang, S. (2014). Home away from home: International students and their identity-based social networks in Australia. *Journal of International Students,* 4(1), 2-15. DOI: https://doi.org/10.32674/jis.v4i1.493

Goulding, C. (1999). Consumer research, interpretive paradigms and methodological ambiguities. *European Journal of Marketing*, *33*(9/10), 859-873 https://doi.org/10.1108/03090569910285805

Gonzalez, M. (2024, August 29). OU Police Department warns students of season ticket scam. *KFOR.com.* https://kfor.com/news/local/ou-police-department-warns-students-of-season-ticket-scam/

Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. *Handbook of qualitative research*, *2*(163-194), 105. https://miguelangelmartinez.net/IMG/pdf/1994_Guba_Lincoln_Paradigms_Quali_Research_chapter.pdf

Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. *Field methods,* 18(1), 59-82. https://doi.org/10.1177/1525822X0527990

Gulati, R. (2003). The threat of social engineering and your defense against it. *SANS Institute InfoSec Reading Room*. http://www.sans.org/rr/papers/index.php?id=1232

Gurung, A., & Raja, M. K. (2016). Online privacy and security concerns of consumers. *Information & Computer Security*, *24*(4), 348-371. https://doi.org/10.1108/ICS-05-2015-0020

Hanson, A. (2017). Negative case analysis. *The international encyclopedia of communication research methods*, 1-2. https://doi.org/10.1002/9781118901731.iecrm0165

Harmon-Jones, E., & Allen, J. J. (2001). The role of affect in the mere exposure effect: Evidence from psychophysiological and individual differences approaches. *Personality and Social Psychology Bulletin,* 27(7), 889-898. https://doi.org/10.1177/0146167201277011

Hasham, S., Joshi, S., & Mikkelsen, D. (2019, October 1). Financial crime and fraud in the age of cybersecurity. McKinsey & Company. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/financial-crime-and-fraud-in-the-age-of-cybersecurity#/

Harris, A., Parke, A., & Griffiths, M. D. (2018). The case for using personally relevant and emotionally stimulating gambling messages as a gambling harm-minimisation strategy. *International Journal of Mental Health and Addiction*, 16, 266-275. https://doi.org/10.1007/s11469-016-9698-7

Hazari, S., Hargrave, W., & Clenney, B. (2008). An empirical investigation of factors influencing information security behavior. *Journal of Information Privacy and Security,* 4(4), 3-20. https://doi.org/10.1080/2333696X.2008.10855849

Halder, D., & Jaishankar, K. (Eds.). (2011). *Cybercrime and the victimization of women: Laws, rights, and regulations: Laws, rights, and regulations*. Igi Global.

Hadnagy, C. (2010). *Social engineering: The art of human hacking*. John Wiley & Sons. http://localhost/handle/Hannan/1327

Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers & Security*, *73*, 102-113. https://doi.org/10.1016/j.cose.2017.10.008

Härtel, C. E., & Panipucci, D. (2007). Chapter 12 How 'bad apples' spoil the bunch: Faultlines, emotional levers, and exclusion in the workplace. In *Functionality, Intentionality and Morality* (pp. 287-310). Emerald Group Publishing Limited. https://doi.org/10.1016/S1746-9791(07)03012-X

Hayes, A. F., & Krippendorff, K. (2007). Answering the call for a standard reliability measure for coding data. *Communication methods and measures*, *1*(1), 77-89. https://doi.org/10.1080/19312450709336664

Hall, B. F. (2002). A new model for measuring advertising effectiveness. *Journal of Advertising Research*, 42(2), 23-31. https://doi.org/10.2501/JAR-42-2-23-31

Hadnagy, C., & Kelly, P. F. (2014). Unmasking the Social Engineer: *The Human Element of Security*. John Wiley & Sons.

Hargittai, E. (2007). Whose space? Differences among users and non-users of social network sites. *Journal of computer-mediated communication*, *13*(1), 276-297. https://doi.org/10.1111/j.1083-6101.2007.00396.x

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

Heim, T. N. (2023). *Global governance and regulation of cybersecurity: Towards coherence or fragmentation?* [PhD Thesis - Research UT, graduation UT, University of Twente]. University of Twente. https://doi.org/10.3990/1.9789036556248

Heyn, M. E. (2013). *Experiences of male Saudi Arabian international students in the United States*. Western Michigan University.

Hinyard, L. J., & Kreuter, M. W. (2007). Using narrative communication as a tool for health behavior change: a conceptual, theoretical, and empirical overview. *Health education & behavior*, *34*(5), 777-792. https://doi.org/10.1177/1090198106291963

Hinson, G. (2008). Social engineering techniques, risks, and controls. *EDPAC: The EDP Audit, Control, and Security Newsletter*, *37*(4-5), 32-46. https://doi.org/10.1080/07366980801907540

Hofstede, G. (2001). Culture's consequences: Comparing values, behaviors, institutions and organizations across nations. *Thousand Oaks*.

Hofstede, G. (1980). Culture and organizations. *International studies of management & organization*, *10*(4), 15-41. https://doi.org/10.1080/00208825.1980.11656300

Hofer, V. J. (2009). *The identification of issues serving as barriers to positive educational experiences for Saudi Arabian students studying in the state of Missouri*. University of Missouri-Saint Louis.

Hong, W., Chan, F. K., & Thong, J. Y. (2021). Drivers and inhibitors of internet privacy concern: a multidimensional development theory perspective. *Journal of Business Ethics*, *168*(3), 539-564. https://doi.org/10.1007/s10551-019-04237-1

Horstman, H. K., Jordan, E., & Yue, J. (2023). Memorable Messages in Families. In Oxford *Research Encyclopedia of Communication.* https://doi.org/10.1093/acrefore/9780190228613.013.1444

Hofstede, G. (2001). Culture's consequences: Comparing values, behaviors, institutions and organizations across nations. *Thousand Oaks*.

Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2008). Low self-control, routine activities, and fraud victimization. *Criminology*, *46*(1), 189-220. https://doi.org/10.1111/j.1745-9125.2008.00101.x

Hornik, R., & Kelly, B. (2007). Communication and diet: an overview of experience and principles. *Journal of nutrition education and behavior,* 39(2), S5-S12.https://doi.org/10.1016/j.jneb.2006.08.020

Hsieh, H. F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research*, 15(9), 1277-1288.

Huang, W., & Brockman, A. (2011). Social engineering exploitations in online communications: Examining persuasions used in fraudulent e-mails. *Crime online: Correlates, causes, and context,* 87-111.

Hull, M., Zhang-Kennedy, L., Baig, K., & Chiasson, S. (2022). Understanding individual differences: factors affecting secure computer behaviour. *Behaviour & Information Technology*, 41(15), 3237-3263. https://doi.org/10.1080/0144929X.2021.1977849

Ion, I., Reeder, R., & Consolvo, S. (2015). {"... No} one Can Hack My {Mind"}: Comparing Expert and {Non-Expert} Security Practices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)* (pp. 327-346). https://www.usenix.org/system/files/conference/soups2015/soups15-paper-ion.pdf

Işık, Ö., Chatterjee, D., & Lourenço, D. A. (2024, July 8). *Getting Cybersecurity Right*. California Management Review. https://cmr.berkeley.edu/2024/07/getting-cybersecurity-right/

Jakobsson, M., & Ratkiewicz, J. (2006, May). Designing ethical phishing experiments: a study of (ROT13) rOnl query features. *In Proceedings of the 15th International Conference on World Wide Web* (pp. 513-522). https://doi.org/10.1145/1135777.1135853

Jamshed, S. (2014). Qualitative research method-interviewing and observation. *Journal of basic and clinical pharmacy*, 5(4), 87. https://doi.org/10.4103/0976-0105.141942

Janesick, V. J. (1994). The dance of qualitative research design: Metaphor, methodolatry, and meaning. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of qualitative research* (pp. 209– 219). Sage Publications, Inc. https://psycnet.apa.org/record/1994-98625-011

Jebb, A. T., Parrigon, S., & Woo, S. E. (2017). Exploratory data analysis as a foundation of inductive research. Human resource management review, 27(2), 265-276. https://doi.org/10.1016/j.hrmr.2016.08.003

Kahneman, D., & Frederick, S. (2005). A Model of Heuristic Judgment. In K. J. Holyoak & R. G. Morrison (Eds.), *The Cambridge handbook of thinking and reasoning* (pp. 267–293). Cambridge University Press.

Kaufmann, R., Vallade, J. I., & Frisby, B. N. (2021). Memorable messages in times of uncertainty: Communicative strategies to encourage motivation and connection. *Communication Education*, *70*(3), 288-306. https://doi.org/10.1080/03634523.2021.1904144

Kallio, H., Pietilä, A. M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. *Journal of advanced nursing*, *72*(12), 2954-2965. https://doi.org/10.1111/jan.13031

Kennedy, J. P., Rorie, M., & Benson, M. L. (2021). COVID-19 frauds: An exploratory study of victimization during a global crisis. *Criminology & Public Policy*, *20*(3), 493-543. https://doi.org/10.1111/1745-9133.12554

Kerley, K. R., & Copes, H. (2002). Personal fraud victims and their official responses to victimization. *Journal of Police and Criminal Psychology*, *17*(1), 19-35. https://doi.org/10.1007/BF02802859

Keyton, J., Bisel, R. S., & Ozley, R. (2009). Recasting the link between applied and theory research: Using applied findings to advance communication theory development. *Communication Theory,* 19(2), 146-160. https://doi.org/10.1111/j.1468-2885.2009.01339.x

Kirova, D., & Baumöl, U. (2018). Factors that affect the success of security education, training, and awareness programs: A literature review. *Journal of Information Technology Theory and Application (JITTA)*, *19*(4), 4. https://aisel.aisnet.org/jitta/vol19/iss4/4

Kim, J., Park, J., & Son, S. (2021). The Abuser Inside Apps: Finding the Culprit Committing Mobile Ad Fraud. In *NDSS*. https://dx.doi.org/10.14722/ndss.2021.23161

Klein, H. A., Lin, M. H., Miller, N. L., Militello, L. G., Lyons, J. B., & Finkeldey, J. G. (2019). Trust across culture and context. *Journal of Cognitive Engineering and Decision Making*, *13*(1), 10-29. https://doi.org/10.1177/1555343418810936

Knapp, M. L., Stohl, C., & Reardon, K. K. (1981). "Memorable" messages. *Journal of Communication*, 31(4), 27-41.https://doi.org/10.1111/j.1460-2466.1981.tb00448.x

Kreuter, M. W., Green, M. C., Cappella, J. N., Slater, M. D., Wise, M. E., Storey, D., ... & Woolley, S. (2007). Narrative communication in cancer prevention and control: A framework to guide research and application. *Annals of behavioral medicine*, *33*, 221-235. https://doi.org/10.1007/BF02879904

Krebs, B. (2014). Spam nation: The inside story of organized cybercrime-from global epidemic to your front door. Sourcebooks, Inc.

Kshetri, N. (2010). The global cybercrime industry: economic, institutional and strategic perspectives. *Springer Science & Business Media.*

Kumar, N., Mohan, K., & Holowczak, R. (2008). Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls. *Decision Support Systems*, *46*(1), 254-264. https://doi.org/10.1016/j.dss.2008.06.010

Kuang, K., Tian, Z., Wilson, S. R., & Buzzanell, P. M. (2023). Memorable messages as anticipatory resilience: Examining associations among memorable messages, communication resilience processes, and mental health. Health communication, 38(6), 1136-1145. https://doi.org/10.1080/10410236.2021.1993585

Kumar, S. (2022). An Analysis Of Phreaking as Sight of Cybercrime. *International Research Journal of Modernization in Engineering Technology and Science,* 2582-5208 https://www.researchgate.net/publication/360726171

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L.F., Hong, J. and Nunge, E. (2007), "Protecting people from phishing: the design and evaluation of an embedded training email system," Conference on Human Factors in Computing Systems – Proceedings, pp. 905-914, https://doi.org/10.1145/1240624.1240760

LaDonna, K. A., Taylor, T., & Lingard, L. (2018). Why open-ended survey questions are unlikely to support rigorous qualitative insights. *Academic Medicine*, *93*(3), 347-349. https://doi.org/10.1097/ACM.0000000000002088

Langenderfer, J., & Shimp, T. A. (2001). Consumer vulnerability to scams, swindles, and fraud: A new theory of visceral influences on persuasion. *Psychology & Marketing,* 18(7), 763-783. https://doi.org/10.1002/mar.1029

Lang, A. (2000). The limited capacity model of mediated message processing. *Journal of communication,* 50(1), 46-70. https://doi.org/10.1111/j.1460-2466.2000.tb02833.x

Lefdahl-Davis, E. M., & Perrone-McGovern, K. M. (2015). The cultural adjustment of Saudi women international students: A qualitative examination. *Journal of Cross-Cultural Psychology*, *46*(3), 406-434. https://doi.org/10.1177/0022022114566680

Lewis, S. (2015). Qualitative inquiry and research design: Choosing among five approaches. *Health promotion practice*, *16*(4), 473-475. https://doi.org/10.1177/1524839915580941

Lewis, M. A., McBride, C. M., Pollak, K. I., Puleo, E., Butterfield, R. M., & Emmons, K. M. (2006). Understanding health behavior change among couples: An interdependence and communal coping approach. *Social science & medicine,* 62(6), 1369-1380. https://doi.org/10.1016/j.socscimed.2005.08.006

Lee, Y., & Kozar, K. A. (2005). Investigating factors affecting the adoption of anti-spyware systems. *Communications of the ACM*, *48*(8), 72-77. https://doi.org/10.1145/1076211.1076243

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, *18*(2), 177-187. https://doi.org/10.1057/ejis.2009.11

Leonard, E. A. (2022). An Examination of Minnesota Multiphasic Personality Inventory-3 (MMPI-3) Profiles of International Saudi Arabian College Students. https://repository.fit.edu/etd/400/

Lewin, S. (2015). Can sociological thinking help to address the bad apples and rotten barrels of the financial industry?. *Researching Sociology*. http://blogs.lse.ac.uk/researchingsociology/

Levine, S. (2021, November 18). *FTC analysis shows COVID fraud thriving on social media platforms*. Federal Trade Commission. https://www.ftc.gov/business-guidance/blog/2021/11/ftc-analysis-shows-covid-fraud-thriving-social-media-platforms

Lincoln, Y. S., Guba, E. G. (1985). *Naturalistic Inquiry.* India: SAGE Publications.

Lincoln, Y. S., & Guba, E. G. (1986). But is it rigorous? Trustworthiness and authenticity in naturalistic evaluation. *New directions for program evaluation,* 1986(30), 73-84. https://doi.org/10.1002/ev.1427

Liginlal, D., Sim, I., & Khansa, L. (2009). How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *computers & security*, *28*(3-4), 215-228. https://doi.org/10.1016/j.cose.2008.11.003

Lincoln, Y. S., & Guba, E. G. (1988). Criteria for Assessing Naturalistic Inquiries as Reports. https://files.eric.ed.gov/fulltext/ED297007.pdf

Long, D. E. (2005). *Culture and customs of Saudi Arabia*. Greenwood Press.

Loewenstein, G. F., Hsee, C. K., Weber, E. U., & Welch, N. (2001). Risk as Feelings. *Psychological Bulletin*, *127*(2), 267-286. https://doi.org/10.1037/0033-2909.127.2.267

Lopez, S. J., Pedrotti, J. T., & Snyder, C. R. (2018*). Positive psychology: The scientific and practical explorations of human strengths*. Sage publications.

Looker, E. D., Denton, M. A., & Davis, C. K. (1989). Bridging the gap: Incorporating qualitative data into quantitative analyses. *Social Science Research*, *18*(4), 313-330. https://doi.org/10.1016/0049-089X(89)90011-2

Lucas, K., & Buzzanell, P. M. (2012). Memorable messages of hard times: Constructing short- and long-term resiliencies through family communication. *Journal of Family Communication*, *12*(3), 189-208. https://doi.org/10.1080/15267431.2012.687196

Lusardi, A., & Mitchell, O. S. (2014). The economic importance of financial literacy: Theory and evidence. *American Economic Journal: Journal of Economic Literature,* 52(1), 5-44. https://www.aeaweb.org/articles?id=10.1257/jel.52.1.5

Mandell, L., & Klein, L. S. (2009). The impact of financial literacy education on subsequent financial behavior. *Journal of Financial Counseling and planning*, 20(1). https://ssrn.com/abstract=2224231

Mann, I. (2017). *Hacking the human: social engineering techniques and security countermeasures.* Routledge.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of experimental social psychology*,19(5), 469-479. https://doi.org/10.1016/0022-1031(83)90023-9

Marginson, S. (2012). *International student security.* The SAGE handbook of international higher education, 207-221.

Mahanta, K., & Maringanti, H. B. (2023). *Social Engineering Attacks and Countermeasures* (pp. 307–337). igi global. https://doi.org/10.4018/978-1-6684-8218-6.ch013

Mathkur, N. M. M. (2019). *Assessing the business ethics of Saudi Arabian Islamic banking sector: an analysis of banks' employees and customers perspectives* (Doctoral dissertation, University of Bolton). https://core.ac.uk/download/pdf/301022014.pdf

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of management review*, *20*(3), 709-734. https://doi.org/10.5465/amr.1995.9508080335

Ma, K. W. F., & McKinnon, T. (2021). COVID-19 and cyber fraud: Emerging threats during the pandemic. *Journal of Financial Crime*, *29*(2), 433-446. https://doi.org/10.2139/ssrn.3718845

Maurer DW (1940/1999) *The Big Con: The Story of the Confidence Man*. New York: Anchor.

Manske, K. (2000). An introduction to social engineering. *Information Systems Security*, 9, 53-60. https://doi.org/10.1201/1086/43312.9.5.20001112/31378.10

Merriam, S. B., & Tisdell, E. J. (2009). Dealing with validity, reliability, and ethics. *Qualitative research: A guide to design and implementation,* 209-235. http://ereserve.library.utah.edu/Annual/ELP/7960/Rorrer/elp7960dealing.pdf

Messick, D. M., & Bazerman, M. H. (1996). Ethical leadership and the psychology of decision making. *MIT Sloan Management Review*. https://sloanreview.mit.edu/article/ethical-leadership-and-the-psychology-of-decision-making/

Merolla, A. J., Beck, G. A., & Jones, A. (2017). Memorable Messages as Sources of Hope. *Communication Quarterly*, *65*(4), 456–480. https://doi.org/10.1080/01463373.2017.1288149

McQuail, D. (2010). *McQuail's mass communication theory*. Sage publications.

McNicholas, T., & Smith Randolph, W. (2024, February 15). *CBS New York Investigates "spoofing" scams after nurse loses life savings*. *CBS News.* https://www.cbsnews.com/newyork/news/cbs-new-york-investigates-spoofing-scams-after-nurse-loses-life-savings/

Milletary, J., & Center, C. C. (2005). Technical trends in phishing attacks. *Retrieved December,* 1(2007), 3-3. https://www.cisa.gov/sites/default/files/publications/phishing_trends0511.pdf

Ministry of Education, Saudi Arabia. (n.d.). *Statistics portal*. Safeer. Retrieved December 4, 2024, from https://safeer2.moe.gov.sa/Portal/Statistics.

Ministry of Education. (n.d.). *Statistics*. Safeer2. Retrieved November 1, 2024, from https://safeer2.moe.gov.sa/Portal/Statistics

Mitnick, K. D., & Simon, W. L. (2003). *The art of deception: Controlling the human element of security*. John Wiley & Sons. https://www.angelfire.com/psy/rokito/mitnickdeception.pdf

Michel, M. C. K., & King, M. C. (2019, November). Cyber influence of human behavior: personal and national security, privacy, and fraud awareness to prevent harm. In *2019 IEEE International Symposium on Technology and Society (ISTAS)*(pp. 1-7). IEEE https://doi.org/10.1109/ISTAS48451.2019.8938009

Miczo, N., Danhour, E., Lester, K. E., & Bryant, J. (2013). Memorable messages and the H1N1 flu virus. *Western Journal of Communication,* 77(5), 625–644. https://doi.org/10.1080/10570314.2013.776099

Morse, J. M. (1995). The significance of saturation. *Qualitative health research*, *5*(2), 147-149. doi:10.1177/104973239500500201

Moore, T., & Clayton, R. (2007, June). An Empirical Analysis of the Current State of Phishing Attack and Defence. *In WEIS.* https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=8b2ec983f6a730ce936a258aa181066e59b67651

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security*, *59*, 186-209. https://doi.org/10.1016/j.cose.2016.03.004

Moussaoui, L. S., Claxton, N., & Desrichard, O. (2021). Fear appeals to promote better health behaviors: an investigation of potential mediators. Health Psychology and Behavioral Medicine, 9(1), 600-618. https://doi.org/10.1080/21642850.2021.1947290

Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The role of user behaviour in improving cyber security management. *Frontiers in Psychology*, *12*, 561011. https://doi.org/10.3389/fpsyg.2021.561011

Moore, R. (2010). *Cybercrime: Investigating High-Technology Computer Crime* (2nd ed.). Routledge. https://doi.org/10.4324/9781315721767

Mousa, S. (2019). Cyber security: Exploring awareness among university students at a public educational institution. *International Journal of Innovative Research and Knowledge*, *4*(5), 88-97.

Mwagwabi, F., & Jiow, J. H. (2021). Compliance with security guidelines in teenagers: the conflicting role of peer influence and personal norms. *Australasian Journal of Information Systems*, *25*. https://doi.org/10.3127/ajis.v25i0.2953

Mwagwabi, F., McGill, T., & Dixon, M. (2018). Short-term and long-term effects of fear appeals in improving compliance with password guidelines. *Communications of the Association for Information Systems*, *42*(1), 7. https://doi.org/10.17705/1CAIS.04207

Nazione, S., Laplante, C., Smith, S. W., Cornacchione, J., Russell, J., & Stohl, C. (2011). Memorable Messages for Navigating College Life. *Journal of Applied Communication Research*, *39*(2), 123–143. https://doi.org/10.1080/00909882.2011.556138

Niederdeppe, J. (2014). Conceptual, empirical, and practical issues in developing valid measures of public communication campaign exposure. *Communication Methods and Measures,* 8(2), 138-161. https://doi.org/10.1080/19312458.2014.903391

Nickerson, M. A. (2019). Fraud in a world of advanced technologies: The possibilities are (unfortunately) endless. *The CPA Journal*, *89*(6), 28-34. https://login.ezproxy.lib.ou.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fscholarly-journals%2Ffraud-world-advanced-technologies-possibilities%2Fdocview%2F2239576995%2Fse-2%3Faccountid%3D12964

Noar, S. M. (2006). A 10-year retrospective of research in health mass media campaigns: Where do we go from here? *Journal of Health Communication,* 11(1), 21-42. https://doi.org/10.1080/10810730500461059

Noar, S. M., & Zimmerman, R. S. (2005). Health Behavior Theory and cumulative knowledge regarding health behaviors: are we moving in the right direction?. *Health education research*, 20(3), 275-290. https://doi.org/10.1093/her/cyg113

Nobles, C. (2021). *Banking cybersecurity culture influences on phishing susceptibility*. Temple University.

Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. *Evidence-based nursing*, *18*(2), 34-35. https://doi.org/10.1136/eb-2015-102054

Ogata Jones, K., Denham, B. E., & Springston, J. K. (2006). Effects of mass and interpersonal communication on breast cancer screening: Advancing agenda-setting theory in health contexts. *Journal of Applied Communication Research,*34(1), 94-113. https://doi.org/10.1080/00909880500420242

Orrego Dunleavy, V., & Yang, Q. (2015). Memorable messages and newcomer socialization on campus: Messages about body image among student athletes, sorority members, and freshmen. *Communication Research Reports*, *32*(3), 225-238. https://doi.org/10.1080/08824096.2015.1052902

Othman, R., Aris, N. A., Mardziyah, A., Zainan, N., & Amin, N. M. (2015). Fraud detection and prevention methods in the Malaysian public sector: Accountants' and internal auditors' perceptions. *Procedia Economics and Finance*, 28, 59-67. https://doi.org/10.1016/S2212-5671(15)01082-5

Oxford English Dictionary. (2023). *Social engineering (n.), sense 2*. https://doi.org/10.1093/OED/9026002772

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & security,* 42, 165-176 https://doi.org/10.1016/j.cose.2013.12.003

Parr, G., Bradley, L., & Bingi, R. (1992). Concerns and feelings of international students. *Journal of College Student Development, 33*(1), 20–25. https://psycnet.apa.org/record/1992-29282-001

Patton, M. Q. (1987). *How to use qualitative methods in evaluation* (No. 4). Sage.

Parsons, K., McCormac, A., Pattinson, M. R., Butavicius, M. A., & Jerram, C. (2013). An Analysis of Information Security Vulnerabilities at Three Australian Government Organisations. In *EISMC* (pp. 34-44).

Parsons, K., McCormac, A., Butavicius, M., & Ferguson, L. (2010). *Human factors and information security: individual, culture and security environment*.

Patton, M. Q. (2014). *Qualitative research & evaluation methods: Integrating theory and practice*. Sage publications.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2014). A study of information security awareness in Australian government organisations. *Information Management & Computer Security,* 22(4), 334-345. https://doi.org/10.1108/IMCS-10-2013-0078

Petty, R. E., & Cacioppo, J. T. (1986). Communication and persuasion: Central and peripheral routes to attitude change. *Springer-Verlag.* https://doi.org/10.1007/978-1-4612-4964-1

Pervaiz, F., Nawaz, R. S., Ramzan, M. U., Usmani, M. Z., Mare, S., Heimerl, K., ... & Razaq, L. (2019, July). An assessment of SMS fraud in Pakistan. *In Proceedings of the 2nd ACM SIGCAS Conference on Computing and Sustainable Societies* (pp. 195-205). https://dl.acm.org/doi/10.1145/3314344.3332500

Peltier, T. R. (2006). Social engineering: Concepts and solutions. *Information Systems Security, 15*(5), 13-21. https://login.ezproxy.lib.ou.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fscholarly-journals%2Fsocial-engineering-concepts-solutions%2Fdocview%2F229581839%2Fse-2%3Faccountid%3D12964

Phelps E. A. (2004). Human emotion and memory: interactions of the amygdala and hippocampal complex. *Current opinion in neurobiology*, *14*(2), 198–202. https://doi.org/10.1016/j.conb.2004.03.015

Philipsen, G. (1992). *Speaking culturally: Explorations in social communication*. Suny Press.

Ploderer, B., Reitberger, W., Oinas-Kukkonen, H., & van Gemert-Pijnen, J. (2014). Social interaction and reflection for behaviour change. *Personal and ubiquitous computing*, 18, 1667-1676. https://doi.org/10.1007/s00779-014-0779-y

Popping, R. (2015). Analyzing open-ended questions by means of text analysis procedures. *Bulletin of Sociological Methodology/Bulletin de Méthodologie Sociologique*, *128*(1), 23-39. https://doi.org/10.1177/0759106315597389

Pratt, M. G. (2009). From the editors: For the lack of a boilerplate: Tips on writing up (and reviewing) qualitative research. *Academy of management journal*, *52*(5), 856-862. https://doi.org/10.5465/amj.2009.44632557

Puram, P. K., Kaparthi, M., & Rayaprolu, A. K. H. (2011). Online scams: Taking the fun out of the internet. Indian Journal of Computer Science and Engineering, 2(4), 559-565. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=e51e9413f0879747b6b9ad73146498639d357059

Raman, K. (2008). Ask and you will receive. *Mcafee Security Journal*, 9-12.

Ramamoorti, S. (2008). The psychology and sociology of fraud: Integrating the behavioral sciences component into fraud and forensic accounting curricula. *Issues in accounting education*, *23*(4). http://jthomasniu.org/class/781/Readings/psychoffraud.pdf

Rahman, M. R. A. (2020). Online Scammers and Their Mules in Malaysia. *Malaysian Journal of Law & Society*, *26*. https://doi.org./10.17576/juum-2020-26-08

Razaq, L., Ahmad, T., Ibtasam, S., Ramzan, U., & Mare, S. (2021). " We Even Borrowed Money From Our Neighbor" Understanding Mobile-based Frauds Through Victims' Experiences. *Proceedings of the ACM on human-computer interaction*, *5*(CSCW1), 1-30. https://dl.acm.org/doi/10.1145/3449115

Rainie, L., Kiesler, S., Kang, R., Madden, M., Duggan, M., Brown, S., & Dabbish, L. (2013). Anonymity, privacy, and security online. *Pew research center*, *5*. http://pewinternet.org/Reports/2013/Anonymity-online.aspx

Rabianski, J. S. (2003). Primary and secondary data: Concepts, concerns, errors, and issues. *The Appraisal Journal, 71*(1), 43-55. https://login.ezproxy.lib.ou.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fscholarly-journals%2Fprimary-secondary-data-concepts-concerns-errors%2Fdocview%2F199981547%2Fse-2%3Faccountid%3D12964

Redmiles, Elissa M., Sean Kross, and Michelle L. Mazurek. "How i learned to be secure: a census-representative survey of security advice sources and behavior." In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pp. 666-677. 2016. https://doi.org/10.1145/2976749.2978307

Rebovich, D. J., Layne, J., Jiandani, J., & Hage, S. (2000). *The national public survey on white collar crime* (pp. 1-45). Morgantown, WV: National White Collar Crime Center. https://www.ojp.gov/pdffiles1/Digitization/181968NCJRS.pdf

Redmiles, E. M., Malone, A. R., & Mazurek, M. L. (2016, May). I think they're trying to tell me something: Advice sources and selection for digital security. In *2016 IEEE Symposium on Security and Privacy (SP)* (pp. 272-288). IEEE. DOI**:** 10.1109/SP.2016.24

Rege, A., Williams, K., & Mendlein, A. (2019, June). A social engineering course project for undergraduate students across multiple disciplines. In *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* (pp. 1-8). IEEE. 10.1109/CyberSecPODS.2019.8885085

Revilla, M., Couper, M. P., & Ochoa, C. (2019). Willingness of online panelists to perform additional tasks. *Methods, data, analyses: a journal for quantitative methods and survey methodology (mda)*, *13*(2), 223-252. https://doi.org/10.12758/mda.2018.01

Rivis, A., & Sheeran, P. (2003). Descriptive norms as an additional predictor in the theory of planned behaviour: A meta-analysis. *Current psychology*, *22*, 218-233. https://doi.org/10.1007/s12144-003-1018-2

Rieber, E. (2024). *Vulnerability to online fraud-A mixed-method study of human factors, user perceptions and strategies*(Master's thesis, NTNU). https://hdl.handle.net/11250/3157963

Rosenstock, I. M. (2005). Why people use health services. *The Milbank Quarterly*, 83(4). doi: 10.1111/j.1468-0009.2005.00425.x

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The journal of psychology*, 91(1), 93-114. https://doi.org/10.1080/00223980.1975.9915803

Rogers, E. M. (1995). *Diffusion of innovations* (4th ed.). New York: Free Press.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social psychology: A source book*, 153-176.

Rosenstock, I. M. (1974). Historical origins of the health belief model. *The Health Belief Model and personal health behavior/Charles B*. Slack, Inc. https://doi.org/10.1177/109019817400200403

Saldaña, J. (2021). *The coding manual for qualitative researchers.* Sage Publications Ltd.

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., ... & Jinks, C. (2018). Saturation in qualitative research: exploring its conceptualization and operationalization. *Quality & quantity*, *52*, 1893-1907. https://doi.org/10.1007/s11135-017-0574-8

Saudi university issues warning over rise in online fraud. (2022, April 29). *Arab News.* https://www.arabnews.com/node/2073481/saudi-arabia

Saudi banks launch campaign to raise awareness of financial fraud and ways of prevention. (2017, November 26). *Saudigazette*. https://saudigazette.com.sa/article/522758

Sawir, E., Marginson, S., Deumert, A., Nyland, C., & Ramia, G. (2008). Loneliness and international students: An Australian study. *Journal of studies in international education,* 12(2), 148-180. https://doi.org/10.1177/1028315307299699

Salik advises customers to stay vigilant of scam emails and social media posts, and clone websites. (2023, April 13). *Eye of Riyadh.*

https://www.eyeofriyadh.com/news/details/salik-advises-customers-to-stay-vigilant-of-scam-emails-and-social-media-posts-and-clone-websites

SAMA issues a guide to combat financial fraud in banks. (2020, August 19). https://sama.gov.sa/en-US/News/Pages/news-598.aspx

SAMA Launches First Edition of Cyber Anti-Fraud Program. (2023, September 19). https://www.sama.gov.sa/en-US/News/Pages/news-980.aspx

SaudiChannelOne. (2022, December 19). طريقة احتيال منتشرة الآن عبر منصات السوشيال ميديا، تعرف عليها. (A scam method that is now widespread across social media platforms, learn about it). [*Video]. YouTube*. https://www.youtube.com/watch?v=XceJWYfSbOs

Schramm, W. (1954). Procedures and effects of mass communication. Teachers College Record, 55(10), 113-138. https://doi.org/10.1177/016146815405501006

Schifter, D. E., & Ajzen, I. (1985). Intention, perceived control, and weight loss: an application of the theory of planned behavior. *Journal of personality and social psychology*, 49(3), 843.

Scown, H. (2019, February 5). Protecting international students from fraud remains a top concern. *Times Higher Education (THE).* https://www.timeshighereducation.com/blog/protecting-international-students-fraud-remains-top-concern

Schneier, B. (2000). Inside risks: semantic network attacks. *Communications of the ACM*, 43(12), 168. https://dl.acm.org/doi/fullHtml/10.1145/355112.355131

Scheier, M. F., & Carver, C. S. (1988). A model of behavioral self-regulation: Translating intention into action. *In Advances in experimental social psychology* (Vol. 21, pp. 303-346). Academic Press. https://doi.org/10.1016/S0065-2601(08)60230-0

Schneier, B. (2000). *Secrets and lies.* New York, NY: John Wiley and Sons.

Shen, Y., & Stringhini, G. (2019). {ATTACK2VEC}: Leveraging temporal word embeddings to understand the evolution of cyberattacks. In *28th USENIX Security Symposium (USENIX Security 19)* (pp. 905-921). https://seclab.bu.edu/papers/attack2vec-usenix2019.pdf

Singh, M. M., Frank, R., & Zainon, W. M. N. W. (2021). Cyber-criminology defense in pervasive environment: A study of cybercrimes in Malaysia. *Bulletin of Electrical Engineering and Informatics*, *10*(3), 1658-1668. DOI: https://doi.org/10.11591/eei.v10i3.3028

Sipayung, E. S. N., Yanti, H. B., & Setya, A. B. (2022, December). Impact of Anti-Fraud Awareness, Fraud Detection Procedures, and Technology to Fraud Detection Skill. *In 3rd Borobudur International Symposium on Humanities and Social Science 2021* (BIS-HSS 2021) (pp. 783-787). Atlantis Press. DOI.10.2991/978-2-494069-49-7_132

Sidor, M., & Dubin, K. (2025, January 28). Past experiences and behavioral change and motivation. *SWEET Institute.* https://sweetinstitute.com/past-experiences-and-behavioral-change-and-motivation/

Siddiqi, M. N. (2004). Riba, bank interest and the rationale of its prohibition. Jeddah: *Islamic Research and Training Institute.* http://ieaoi.ir/files/site1/pages/ketab/english_book/205.pdf

Simulated Phishing Update. (2024, May 13). University of Oklahoma Information Technology. OU IT News. https://www.ou.edu/ouit/news/2024/may/simulated-phishing-update

Slater, M. D. (1997). Persuasion processes across receiver goals and message genres. *Communication Theory*, 7(2), 125-148. https://doi.org/10.1111/j.1468-2885.1997.tb00145.x

Slovic, P. (1978). The psychology of protective behavior. *Journal of Safety Research*, 10(2), 58-68. https://hdl.handle.net/1794/22386

Smith, S., & Butler Ellis, J. (2001). Memorable messages as guides to self-assessment of behavior: An initial investigation. *Communication Monographs*, *68*(2), 154-168. https://doi.org/10.1080/03637750128058

Smith, S. W., Nazione, S., LaPlante, C., Kotowski, M. R., Atkin, C., Skubisz, C. M., & Stohl, C. (2009). Topics and sources of memorable breast cancer messages and their impact on prevention and detection behaviors. *Journal of Health Communication*, 14(3), 293-307. https://doi.org/10.1080/10810730902805903

Smith, S. W., Hamel, L. M., Kotowski, M. R., Nazione, S., LaPlante, C., Atkin, C. K., Stohl, C., & Skubisz, C. (2010). Action tendency emotions evoked by memorable breast cancer messages HEALTH COMMUNICATION 2685 and other associations with prevention and detection behaviors. *Health Communication,* 25(8), 737–746. https://doi.org/10.1080/10410236.2010.521916

Snyder, L. B., & LaCroix, J. M. (2001). How effective are mediated health campaigns. *Public communication campaigns*, 3, 181-190. https://doi.org/10.1080/10810730490271548

Snyder, L. B. (2007). Health communication campaigns and their impact on behavior. *Journal of nutrition education and behavio*r, 39(2), S32-S40. https://doi.org/10.1016/j.jneb.2006.09.004

Social media scams: understanding the consumer experience to create a safer digital world- Consumers International. (2019). https://www.consumersinternational.org/media/293343/social-media-scams-final-245.pdf

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end-user security behaviors. *Computers & Security,* 24(2), 124-133. https://doi.org/10.1016/j.cose.2004.07.001

Steinmetz, K. F., Pimentel, A., & Goe, W. R. (2020). Decrypting social engineering: An analysis of conceptual ambiguity. *Critical Criminology*, *28*, 631-650. https://doi.org/10.1007/s10612-019-09461-9

Stake, R. E. (2008). Qualitative case studies. In N. K. Denzin & Y. S. Lincoln (Eds.), *Strategies of qualitative inquiry* (3rd ed., pp. 119–149). Sage Publications, Inc.

Stohl, C. (1986). The role of memorable messages in the process of organizational socialization. *Communication Quarterly,* 34(3), 231–249. https://doi.org/10.1080/01463378609369638

Strauss, A., & Corbin, J. (1990). *Basics of qualitative research* (Vol. 15). Newbury Park, CA: Sage.

Stokes, D., & Bergin, R. (2006). Methodology or "methodolatry"? An evaluation of focus groups and depth interviews. *Qualitative market research: An international Journal*, *9*(1), 26-37 https://eprints.kingston.ac.uk/id/eprint/677/1/Stokes-D-677.pdf

Steimel, S. (2013). Connecting with volunteers: Memorable messages and volunteer identification. *Communication Research Reports*, 30(1), 12–21. https://doi.org/10.1080/08824096.2012.746220

Strauss, A., & Corbin, J. (1998). *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Thousand Oaks, CA: Sage.

Stebbins, R. A. (2001). *Exploratory research in the social sciences* (Vol. 48). Sage.

Suddaby, R. (2006). From the editors: What grounded theory is not. *Academy of management journal*, *49*(4), 633-642. https://doi.org/10.5465/amj.2006.22083020

Sundar, S. S., Oh, J., Kang, H., & Sreenivasan, A. (2012). How Does Technology Persuade? (chapter 3 pp. 388-404). *SAGE Handbook. Persuas. Dev. Theory Pract.,* 388.

Swedberg, R. (2020). Exploratory research. *The production of knowledge: Enhancing progress in social science*, *2*(1), 17-41.

Thaler, R. H., & Sunstein, C. R. (2008). Nudge: Improving Decisions About Health, Wealth, and Happiness. Yale University Press.

Thomas, D. R. (2006). A general inductive approach for analyzing qualitative evaluation data. *American Journal of Evaluation,* 27(2), 217-233.

Thomas, D. (2002). *Hacker culture*. U of Minnesota Press http://culturehack.org.uk/about/

The psychology of social engineering—the "soft" side of cybercrime. (2020, June 30). Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2020/06/30/psychology-social-engineering-soft-side-cybercrime/

Thornberg, R., & Charmaz, K. (2014). Grounded theory and theoretical coding. *The SAGE handbook of qualitative data analysis*, *5*(2014), 153-69.

Thompson, S. T. (2006). Helping the hacker? Library information, security, and social engineering. *Information Technology and Libraries*, 25(4), 222-225. DOI: https://doi.org/10.6017/ital.v25i4.3355

Thompson, N., McGill, T. J., & Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & security*, *70*, 376-391. https://doi.org/10.1016/j.cose.2017.07.003

Titus, R. M., Heinzelmann, F., & Boyle, J. M. (1995). Victimization of persons by fraud. *Crime & Delinquency*, *41*(1), 54-72. https://doi.org/10.1177/0011128795041001004

Tourangeau, R., Rips, L. J., & Rasinski, K. (Eds.). (2000). *The psychology of survey response.* Cambridge University Press. https://doi.org/10.1017/CBO9780511819322

Tracy, S. J. (2024). *Qualitative research methods: Collecting evidence, crafting analysis, communicating impact*. John Wiley & Sons.

Tracy, S. J. (2010). Qualitative quality: Eight "big-tent" criteria for excellent qualitative research. Qualitative inquiry, 16(10), 837-851. https://doi.org/10.1177/1077800410383121

Tschakert, K. F., & Ngamsuriyaroj, S. (2019). Effectiveness of and user preferences for security awareness training methodologies. *Heliyon,* 5(6). https://doi.org/10.1016/j.heliyon.2019.e02010

Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. Science, 185, 1124-1130. DOI: 10.1126/science.185.4157.1124

Tylor, E. B. (1871). *Primitive culture: researches into the development of mythology, philosophy, religion, art, and custom* (Vol. 2). J. Murray.

Van Steen, T., Norris, E., Atha, K., & Joinson, A. (2020). What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use?. *Journal of Cybersecurity*, *6*(1), tyaa019. https://doi.org/10.1093/cybsec/tyaa019

Van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies*, *123*, 29-39. https://doi.org/10.1016/j.ijhcs.2018.11.003

Varpio, L., Martimianakis, M. A., & Mylopoulos, M. (2022). Qualitative research methodologies: embracing methodological borrowing, shifting and importing. *Researching medical education*, 115-125. https://doi.org/10.1002/9781119839446.ch11

Visa Study Reveals 91% of KSA Consumers Surveyed are at Risk of Responding to Scammers. (2023). Visa. https://sa.visamiddleeast.com/en_SA/about-visa/newsroom/press-releases/prl-18122023.html#:~:text=Visa%20Sponsorships-,Visa%20Study%20Reveals%2091%25%20of%20KSA%20Consumers%20Surveyed%20are%20at,miss%20common%20warnings%20of%20fraud.

Vitak, J., Liao, Y., Subramaniam, M., & Kumar, P. (2018). 'I Knew It Was Too Good to Be True" The Challenges Economically Disadvantaged Internet Users Face in Assessing Trustworthiness, Avoiding Scams, and Developing Self-Efficacy Online. *Proceedings of the ACM on human-computer interaction*, 2(CSCW), 1-25. https://doi.org/10.1145/3274445

Vygotsky, L. S. (1978). *Mind in society: The development of higher psychological processes* (Vol. 86). Harvard university press.

Wash, R., & Rader, E. (2015). Too much knowledge? Security beliefs and protective behaviors among United States internet users. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)* (pp. 309-325). https://www.usenix.org/system/files/conference/soups2015/soups15-paper-wash.pdf

Waldron, V. R., Reutlinger, C., Martin, J., O'Neil, E., & Niess, L. C. (2023). "We are all in this together": Which memorable moral messages guided student responses to the COVID-19 pandemic? *Health Communication,* 1-12. https://doi.org/10.1080/10410236.2023.2286695

Wakefield, M. A., Loken, B., & Hornik, R. C. (2010). Use of mass media campaigns to change health behavior. *The Lancet,* 376(9748), 1261-1271. https://doi.org/10.1016/S0140-6736(10)60809-4

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems,* 18(2), 101- 105. https://doi.org/10.1057/ejis.2009.12

Whiting, L. S. (2008). Semi-structured interviews: guidance for novice researchers. *Nursing Standard* (through 2013), 22(23), 35.

Who experiences scams? A story for all ages. (2022, December 8). Federal Trade Commission. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/12/who-experiences-scams-story-all-ages

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs*, *59*(4), 329-349. https://doi.org/10.1080/03637759209376276

Winnicott, D. W. (1963). The development of the capacity for concern. *Bulletin of the Menninger Clinic*, *27*(4), 167. https://www.proquest.com/openview/dedff87f9567bee06d1ac4584df74455/1?pq-origsite=gscholar&cbl=1818298

Willis, G. B. (2004). *Cognitive interviewing: A tool for improving questionnaire design*. Sage publications. https://www.dima.univr.it/documenti/OccorrenzaIns/matdid/matdid823948.pdf

Wilson, S., Hassan, N. A., Khor, K. K., Sinnappan, S., Abu Bakar, A. R., & Tan, S. A.(2023). A holistic qualitative exploration on the perception of scams, scam techniques and effectiveness of anti-scam campaigns in Malaysia. *Journal of Financial Crime.* DOI:10.1108/JFC-06-2023-0151

Willoughby, J. F., & Noar, S. M. (2022). Fifteen years after a 10-year retrospective: the state of health mass mediated campaigns. *Journal of Health Communication*, *27*(6), 362-374. https://doi.org/10.1080/10810730.2022.2110627

Wilson, C. R. (2021, November 29). What are protective factors in psychology? 36 examples. *PositivePsychology.com*. https://positivepsychology.com/what-are-protective-factors/

Williams Mills, I. (2021). *Western Samoa Students' Experiences of How Culture and Academic Preparation Impacts Educational Success at a U.S. University* (Order No. 28317650). Available from ProQuest Dissertations & Theses Global. (2516202931). https://login.ezproxy.lib.ou.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fdissertations-theses%2Fwestern-samoa-students-experiences-how-culture%2Fdocview%2F2516202931%2Fse-2%3Faccountid%3D12964

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American society for information science and technology*, 59(4), 662-674. https://doi.org/10.1002/asi.20779

Wolff, J. (2018). The real reasons why cybercrimes may be vastly undercounted. *Slate Magazine*, *12*. https://slate.com/technology/2018/02/the-real-reasons-why-cybercrimes-are-vastly-underreported.html

Yazedjian, A., Toews, M.L., Sevin, T., & Purswell, K.E. (2008). "It's a Whole New World": A Qualitative Exploration of College Students' Definitions of and Strategies for College Success. *Journal of College Student Development* 49(2), 141-154. https://doi.org/10.1353/csd.2008.0009.

Yemeni, A. (2023, July 29). *السيرة الذاتية.. احتيال وظيفي جديد يلاحق الباحثين عن العمل عبر وسائل التواصل* (CV...a new job scam that haunts job seekers through social media.). *Makkah newspaper*. https://makkahnewspaper.com/article/1594245

Yiannaka, A. (2023). Food Fraud: a persistent problem that demands a comprehensive approach. *Journal of Consumer Protection and Food Safety,* 18(4), 359–360. https://doi.org/10.1007/s00003-023-01465-6

Yuniarti, R. D., & Ariandi, I. (2017). The effect of internal control and anti-fraud awareness on fraud prevention (A survey on inter-governmental organizations*). Journal of Economics, Business, and Accountancy Ventura*, 20(1), 113-124. https://doi.org/10.14414/jebav.v20i1.751

Zajonc, R. (1968). Attitudinal effects of mere exposure. *Journal of Personality and Social Psychology,* 9, 1-27 https://doi.org/10.1037/h0025848

Zahari, A. I., Bilu, R., & Said, J. (2019). The role of familiarity, trust, and awareness towards online fraud. *Journal of Research and Opinion*, 6(9), 2470-2480. DOI: 10.15520/jro.v6i9.23

Zayid, E. I. M., & Farah, N. A. A. (2017, March). A study on cybercrime awareness test in Saudi Arabia-Alnamas region. In *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)* (pp. 199-202). IEEE. doi: 10.1109/Anti-Cybercrime.2017.7905290.

Zhang, Y., Wu, Q., Zhang, T., & Yang, L. (2022). Vulnerability and fraud: evidence from the COVID-19 pandemic. *Humanities and Social Sciences Communications*, *9*(1), 1-12. https://doi.org/10.1057/s41599-022-01445-5

Zhuang, R., Bardas, A. G., DeLoach, S. A., & Ou, X. (2015, October). A theory of cyber attacks: A step towards analyzing MTD systems. In *Proceedings of the second ACM*

workshop on moving target defense (pp. 11-20). https://doi.org/10.1145/2808475.2808478

Zurko, M. E. (2005, December). User-centered security: Stepping up to the grand challenge. In *21st Annual Computer Security Applications Conference (ACSAC'05)* (pp. 14-pp). IEEE. DOI**:** 10.1109/CSAC.2005.60

62% of Saudis exposed to attempts of financial fraud, survey shows. (2022, April 27). *Saudigazette*. https://www.saudigazette.com.sa/article/619840

Appendix A

The items in the open-ended survey:

1-Please select any of the actions listed below that you have taken to protect your financial and personal information against social engineers' attacks.

Changing passwords more frequently to new ones instead of keeping the same password for a long time (1)
Not using the same password for different accounts (2)
Talking with family members and peers about any fraud-related topic (3)
Hang up and call back using the official number when receiving unexpected calls asking for personal info. (4)
Checking your bank accounts often to spot any strange activity. (5)
Avoid downloading attachments or files until you verify the sources. (6)
Keeping your phone and computer updated with the latest security fixes (7)
Being careful with what you share on social media about yourself (8)
Giving attention to the common fraud tactics (9)
Ignoring requests for money on message apps from known sources. (10)
Other actions please let us know (11)
None of the above (12)

1a- Other actions, please let us know

- - - - - - - - - --- -- -

2-How concerned are you about social engineers' attacks?
Very Concerned (1)

Concerned (2)

Moderately Concerned (3)

Slightly Concerned (4)

Not Concerned at All (5)

2a-Given your level of concern. . .Can you please describe what incidents contribute to your current concern about social engineers' attacks?

- - - - - - - - - --- -- -

3- In the space provided, can you remember a particular instance or source that significantly impacted your concern about social engineers' attacks (e.g., news reports, personal experiences, social media posts, or pee's experiences)?

- - - - - - - - - --- -- -

4- In the space provided, can you remember a time when you recognized a fraud attempt and you avoided or stopped it?

- - - - - - - - - --- -- -

5- In the space provided, please tell a story or more about when a fraud tricked you, a relative, or a friend.

- - - - - - - - - --- -- -

6- In the space provided, please tell us any message, logo, sign, comment, phrase, or word of wisdom that influenced your decision to protect yourself against social engineers' attacks. Please list as many as possible.

7-From all your answers above, which message is most compelling to you regarding avoiding social engineers' attacks? And why?

9- Demographic information

Q1 What is your gender?

Q2 What is your age group?

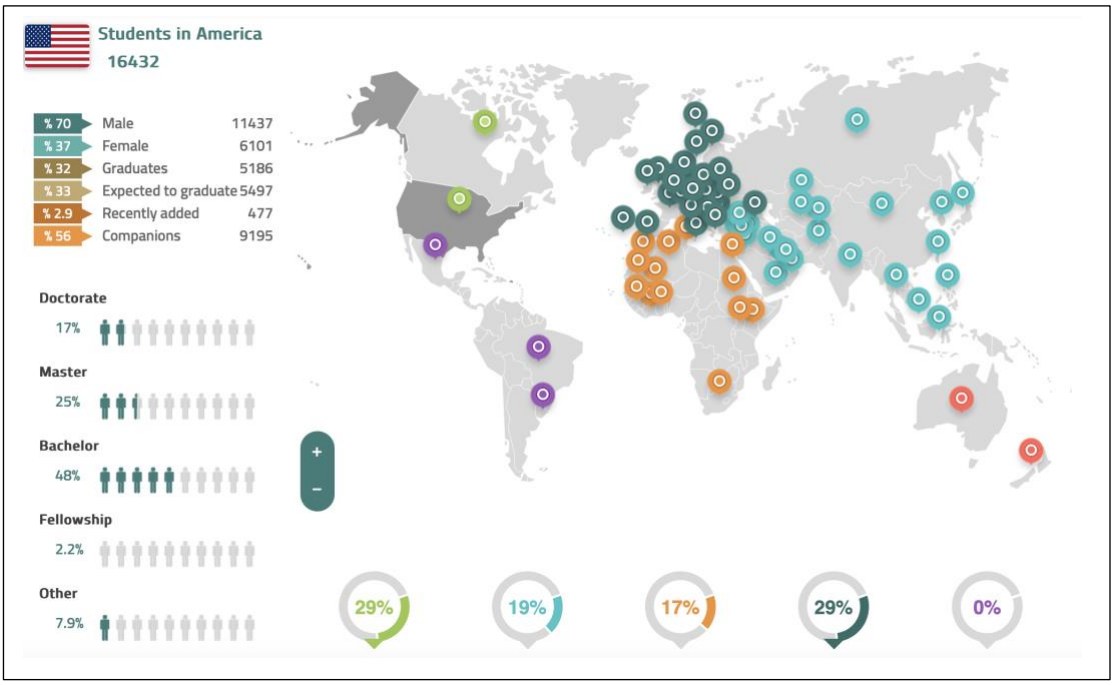
Q3 What is your highest education level?

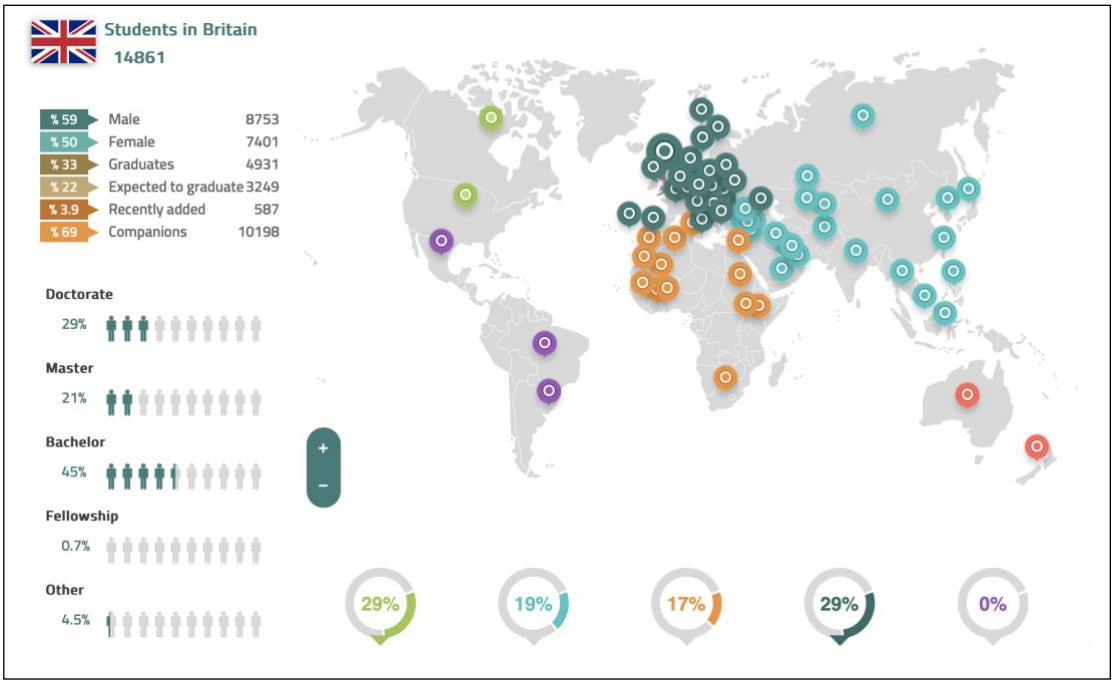
Q4 Which Saudi region are you from?

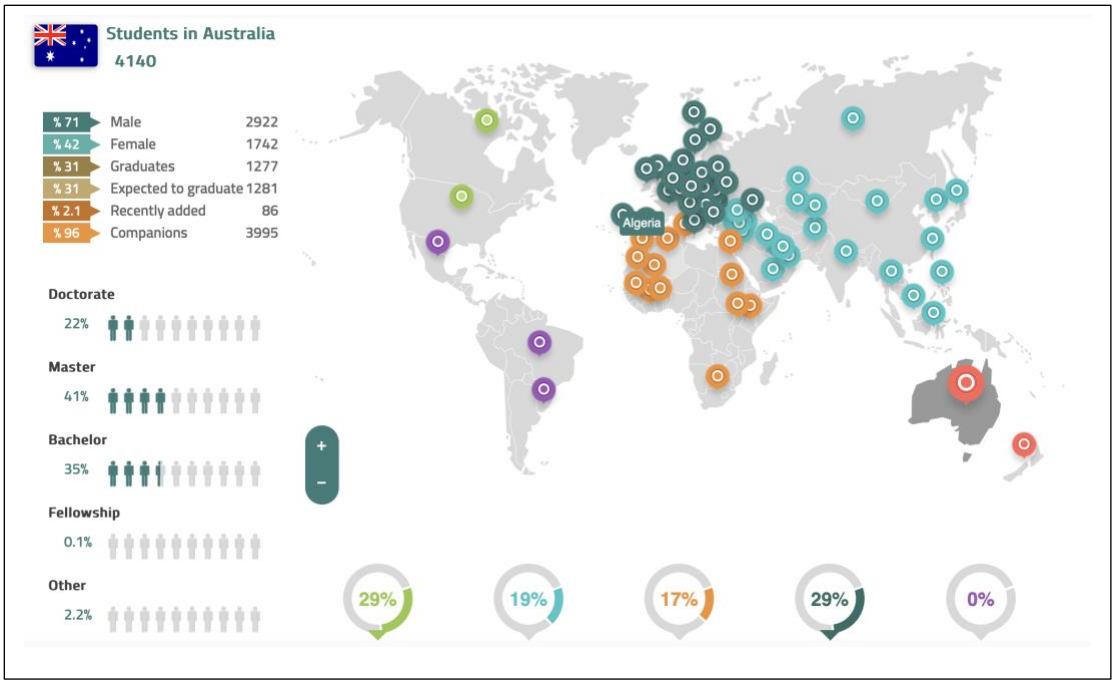
Q5 Which Western country are you currently studying in?

Appendix B

The population of Saudi students studying in Western countries as shown on the Saudi Culture Mission website (Safeer 2)






Students in Australia
4140
%71 Male 2922
%42 Female 1742
%31 Graduates 1277
%31 Expected to graduate 1281
%2.1 Recently added 86
%96 Companions 3995
Doctorate
22%
Master
41%
Bachelor
35%
Fellowship
0.1%
Other
2.2%
Algeria
29%
19%
17%
29%
0%

Appendix C

Initial Coding Table for Open-Ended Responses

Open-coding/ Initial code	Number of evident	Text Responses for the Question Number:
1-Family and friends' negative experiences		
2-Individual, peers' negative experiences		
3-Personal negative experiences		
4-Personal negative experiences abroad		
5-Media messages		
6-Avoidance Strategies		
7-Exploiting advance technology		
8-Authority Warnings		
9-Social media		
10-Suspicious interaction		
11-Word of wisdom		
12-Secure Communication Practices		
13-Awareness of Fraud Tactics		
14-Impersonation of Official Entities		
15-Bank or authority -Warnings		
16-Trust Exploitation		
17-Recalled Educational / training Content		
18-Students who are not Concerned at All		
19-Trust in institutional protection		
20-Do not remember / know		
21-Not applicable		

Appendix D

Focused Coding and Coding Categories

Focused Coding	Number of evident	Text Responses for the Question Number:
1-Family and friends' negative experiences		
2-Individual, peers' negative experiences		
3-Personal negative experiences		
4-Personal negative experiences abroad		
5-Suspicious interaction		
6-Awareness of Fraud Tactics		
7-Avoidance Strategies		
8-Culturally Inspired Word of wisdom		
9-Exploiting advance technology		
10-Authority Warnings		
11- Institutional instruction		
12-media messages		
13-Social media post		
14-Students' self-confidence		
15-Trust in institutional protection		
16-Do not remember / know		
17-Not applicable		

Appendix E

Memorable messages Open Coding

Open-coding/ Initial code	Number of evident	Text Responses for the Question Number:
1- Word of wisdom Cultural References		
2- Avoidance Strategies		
3- Media messages Social media		
4- Bank or authority -Warnings		
5- Do not remember		
6- Recalled Educational / training Content		
7- Not applicable		