Journal of the North for Humanities, Northern Border University, (ISSN: 1658-6999)
Vol. (10) - Issue (1), Part (1) Jan 2025 - Rajab 1446H 35-50

Investigating Risk Factors for Online Fraud Victimization: MIS case study

Mofza Algahtany
Assistant Professor, Department of Management Information System, College of business, Al Bahah University, Kingdom of Saudi Arabia.

(**Received:** 04-03-2024; **Accepted:** 21-05-2024)

Abstract: Enhancing the GDP of Saudi Arabia Kingdom and raising the living standards of the general populace are both greatly aided by the manufacturing sector. Enhancing this sector relies on enhancing the supply chain management performance through strengthening the supply chain capabilities, innovation capabilities, and supply chain agility within this sector. Hence, this study aimed to design a comprehensive model to enhance the SC performance in the manufacturing companies in KSA by examining the SC capabilities, innovation capabilities, and SC agility as strong determinants of the SC performance; a total of 285 questionnaires selected from the manufacturing companies in KSA using a convenience sampling method. The study applied SEM with SMART-PLS 4 to analyze the data collected from the supply chain managers in the KSA manufacturing companies. The study results support all three direct effect hypotheses; the direct impact of the SC capabilities on SC performance, the direct impact of the innovation capabilities on the SC performance and the direct impact of the innovation capabilities on the SC performance. Also, the result of the study supports the mediating impact of the innovation capabilities on the impact of SC capabilities on the SC performance and supports the moderating role of the SC agility on the impact of the innovation capabilities on the SC performance. The study provides very important implications to the supply chain managers in the manufacturing companies in KSA to improve their supply chain performance to gain competitive advantage by applying the model of SC capabilities, innovation capabilities and SC agility in the manufacturing industry.

Keywords: SC Capabilities, Innovation Capabilities, SC Agility, SC Performance, Manufacturing Companies

***

دراسة عوامل الخطر لتعرض الضحايا للاحتيال عبر الإنترنت: دراسة حالة نظم المعلومات الإدارية

مفزع بن سالم القحطاني
أستاذ مساعد، قسم نظم المعلومات الإدارية، كلية الأعمال، جامعة الباحة المملكة العربية السعودية

(**تاريخ الاستلام:** 25-03-2024؛ **تاريخ القبول:** 05-09-2024)

مستخلص البحث: يشير الانتشار الواسع للاحتيال عبر الإنترنت على نطاق عالمي إلى أنه يمثل تهديدًا كبيرًا لاستقرار المجتمعات وأمن ممتلكات الأفراد. هناك عدة عوامل تساهم في احتمال الوقوع ضحية للاحتيال عبر الإنترنت. التحقيق في الرابط بين هذه العوامل والاحتيال عبر الإنترنت يعتبر ذا أهمية قصوى لكشف الأسباب الجذرية له ووضع استراتيجيات وقائية. باستخدام استبيان شمل 723 مشاركًا، استخدمت هذه الدراسة تحليلات أحادية المتغير والانحدار اللوجستي لاستكشاف العوامل المرتبطة بالاحتيال عبر الإنترنت. وُجد أن الجنس، والعمر، والتخصص، والتعليم، والميل للثقة، ونوع الوظيفة، وجاذبية الإعلانات الترويجية لها علاقات إيجابية مع قابلية الاحتيال عبر الإنترنت، بينما كان الوضع الاجتماعي، والدخل، وتفضيل الشراء عبر الإنترنت مرتبطًا سلبًا بالاحتيال عبر الإنترنت.
أكدت التحليلات الإنحدارية اللاحقة أن جميع العوامل المذكورة أعلاه، بما في ذلك جاذبية الإعلانات الترويجية، تعمل كمؤشرات كبيرة للاحتيال عبر الإنترنت. تسلط النموذج النظري والنتائج التجريبية لهذا البحث الضوء على الدور الحاسم الذي يلعبه الاحتيال عبر الإنترنت في جعل الأفراد عرضة للخطر وتساهم في حل الاختلافات الموجودة في الدراسات السابقة بخصوص عوامل الخطر للاحتيال عبر الإنترنت.

كلمات مفتاحية: الاحتيال؛ التسوق عبر الإنترنت؛ الديموغرافيا، الميل للثقة، الاندفاعية.

(*) للمراسلة:
الدكتور مفزع بن سالم القحطاني، أستاذ مساعد، قسم نظم المعلومات الإدارية، كلية الأعمال، جامعة الباحة المملكة العربية السعودية.
البريد الإلكتروني:
m.alqahtani@bu.edu.sa

(*) **Corresponding Author**:
Dr Mofza Algahtany، Assistant Professor, Department of Management Information System, College of business, AL-Baha University, Kingdom of Saudi Arabia.
Email: m.alqahtani@bu.edu.sa

DOI: 10.12816/0062114

1. Introduction

As the digital landscape continues to evolve at an unprecedented rate, the issue of online fraud has emerged as a significant concern, impacting individuals and communities worldwide. This research embarks on a crucial journey to unravel the intricate web of factors contributing to online fraud victimization. With the proliferation of internet usage and the increasing reliance on digital devices, understanding the nuances of online fraud has never been more essential. It is well known that online fraud has caused and continues to cause significant losses in the e-commerce and electronic transactions sector, amounting to tens of billions of dollars globally each year. This remains one of the challenges facing e-commerce. Recently, online and social media fraud has increased in Saudi society. Some studies have mentioned that in Saudi Arabia, where online transactions are highly prevalent, preventing online fraud has become imperative (Alanezi, 2016; Alanezi & Brooks, 2014; Alfuraih, 2008; Aljeaid et al., 2020). There is a scarcity of investigations into online fraud in Saudi Arabia, especially with the rapid technological advancements the country is experiencing. Therefore, reviewing previous research reveals that it focuses on specific aspects such as cybersecurity, the banking sector, or institutions. Consequently, we found it important to study this critical issue at the individual or customer level. Therefore, our study delves deep into the realm of online fraud, aiming to dissect the roles of demographic, psychological, technological, and lifestyle factors in shaping an individual's susceptibility to such scams. In the digital era, where every click, swipe, and download could potentially lead to a fraud trap, it's critical to understand who is most at risk and why. This study seeks to explore this dynamic, focusing on how variables such as age, gender, marital status, education, income, and device usage intertwine to form a complex mosaic of fraud vulnerability. By examining these variables in conjunction with psychological traits like impulsiveness and trust tendency, as well as the impact of negative life events, we aim to provide a comprehensive overview of the factors that increase the likelihood of becoming a victim of online fraud. Moreover, this research is not just academic in nature; it has practical implications for the development of targeted educational programs and strategies to mitigate the risks of online fraud. The goal is to equip the public, particularly in rapidly digitizing societies like Saudi Arabia, with the knowledge and tools necessary to navigate the digital world safely. The criteria mentioned by Shannon et al. (1999) have been taken into consideration in designing this research. By shedding light on the intricate relationship between personal device usage and online fraud vulnerability, this study aims to pave the way for groundbreaking research in this field, offering valuable insights for future preventative measures and policy-making.

Embarking on this research journey, we aspire to uncover the multi-layered facets of online fraud victimization, providing a foundation for future studies and contributing significantly to the global fight against this growing digital menace.

2. Literature review

2.1 Overview of Online Fraud

Internet technology has undergone rapid development and widespread proliferation across the globe (Li, 2023). Estimates indicate that in 2022, losses in the e-commerce sector due to online payment fraud amounted to approximately 41 billion U.S. dollars globally, marking an increase from the previous year. Projections suggest that this figure is set to rise even further to reach 48 billion U.S. dollars by the year 2023 (Pyrkh, 2023). On a global scale, approximately 6.86 cents out of every 100 dollars are lost due to fraudulent activities. In the Single Euro Payments Area (SEPA), roughly 0.24% of all transactions are found to be fraudulent (Van Belle et al., 2023). Various types of social media platforms provide insights into distinct methods of victimization (Lee, 2021). Traditional crimes are swiftly transitioning into non-contact crimes facilitated by telecommunications and the internet.

Additionally, new forms of crimes, such as online fraud, are on the rise (Ni & Wang, 2022). Online fraud has emerged as the primary form of crime that jeopardizes the safety of individuals' lives and property, while also disrupting the order of the digital realm (Fan & Yu, 2022). The Saudi government places significant emphasis on combatting emerging illegal and criminal activities within the telecommunications and internet domain (Sule et al., 2022). Effectively controlling online fraud has become a pressing concern that requires deep reflection and dedicated attention from law enforcement agencies at all levels. However, the scarcity of empirical studies on the factors contributing to online fraud victimization in Saudi Arabia poses a challenge in designing efficient preventive policies and legal initiatives. Consequently, the present study aims to explore the critical factors associated with online fraud in Saudi Arabia, with the goal of assisting the government in formulating intervention programs to mitigate such issues. Recognizing that the interaction between the perpetrator and victim in the context of online fraud plays a crucial role, victimhood itself should be regarded as a risk factor in this type of crime. The concept of "victimity" was initially introduced by Mendelssohn, who defined it as the state, quality, or fact of being a victim (Mendelsohn, 1963).

2.2 Technological Advancements and Fraud Techniques

As the digital landscape rapidly evolves, online fraud has become a major concern, affecting individuals and communities globally. This research sets out on an important mission to explore the complex factors that lead to online fraud victimization. With the widespread use of the internet and growing dependence on digital devices, grasping the intricacies of online fraud is more crucial than ever. For instance, Alonazi (2020) and Alghamdi and Nor (2023) have found that online fraud is steadily increasing in Saudi Arabia, and its techniques have evolved differently in line with the rapid advancement of technology.

2.3 Regional Trends and Specifics in Saudi Arabia

In recent years, Saudi Arabia has witnessed significant development in all fields, especially in technology, where most government transactions and community services can now be conducted online. On the other hand, online fraud has found a fertile environment for targeting victims. Studies and statistics have shown an increase in online fraud (Alghamdi & Nor, 2023; Alonazi, 2020), making such a study particularly important at this time.

The former pertains to various aspects related to the victim, including demographic characteristics, income, online shopping habits, and susceptibility to the influence of promotional advertisements.

When considering these factors of victimity, demographic characteristics are among the risk factors associated with online fraud victimization. Numerous studies have investigated this aspect, but the findings have been varied and inconclusive (Judges et al., 2017; Kadoya et al., 2021; Lang & Riegel, 2023; Ross et al., 2014). As instance, in the research conducted by Fan and Yu (2022) , it was revealed that older age and lower levels of education were linked to an elevated susceptibility to online fraud. In contrast, Whitty (2020) did not find age to be a predictive variable for cyber scam victimization, while education emerged as a positive predictor in the context of online fraud. Parti (2022) reported that higher education did not serve as a protective factor but rather as a predictive factor for online fraud among younger respondents. Additionally, the research conducted by Reyns and Randa (2020) revealed a negative association between age and fraud victimization. Regarding gender, certain studies have proposed that the majority of financial fraud victims are males (Button et al., 2014; Deliema et al., 2020; Whitty, 2020). However, Fan and Yu (2022) reported no significant effects for gender in their findings. The disparities in the existing conclusions may be attributed to variations in the study subjects

and the types of fraud examined. Given its substantial population and the high prevalence of online fraud, a sample study conducted in such a country holds greater representativeness when investigating the risk factors associated with online fraud victimization.

Age, educational attainment, income, the inclination for online shopping, the selection of the digital device (computer or smartphone), and vulnerability to the attraction of promotional advertisements are all significant factors that may contribute to the victimity associated with online fraud. This study in question delved into these factors to investigate their role in contributing to the victimity associated with online fraud. These elements encompass traits like trust tendency and impulsiveness to make purchases influenced by advertisements suggesting that high impulsiveness and elevated risk-taking tendencies are positively correlated with online fraud (Alseadoon et al., 2013; Bossler & Holt, 2010; Mikkola et al., 2020; Ngo & Paternoster, 2011; Norris et al., 2019; Parti, 2022; Pattinson et al., 2011; Williams et al., 2017). According to Mesch and Dodel (2018), individuals who are both trustworthy and impulsive are more likely to participate in online activities and may be more inclined to share personal information. Impulsivity, which is a manifestation of low self-control, is associated with individuals who prioritize immediate gains, often disregarding long-term consequences and the intentions of others (Pratt et al., 2014).

Regarding trust tendency, there is a common belief that more trusting individuals are more likely to fall victim to online fraud. However, findings on trust tendency have been inconsistent. For instance, increased trust was a key factor in the exploitation of older individuals by fraudsters (Ross et al., 2014). Nonetheless, other studies have reported that trust has either a negative impact or no significant effect on fraud victimization(Carter & Weber, 2010; Judges et al., 2017). Therefore, further research is required to comprehensively understand the influence of psychological characteristics such as impulsivity and trust propensity on online fraud victimization.

2.4 The Impact of Social Media

In terms of lifestyle, studies have identified specific lifestyles that can predict fraud victimization. These include lifestyles characterized by extensive internet use, frequent online shopping, habitual responses to electronic messages, and past financial interactions with scammers (Balleisen, 2018; Han et al., 2023; Holtfreter et al., 2008; Parti, 2022; Reisig & Holtfreter, 2013; Vishwanath, 2015). Specific everyday online activities act as positive predictors of cyber victimization by exposing potential victims to cybercriminals (Mesch & Dodel, 2018; Van Wilsem, 2013). The integrated lifestyles and routine activities theory (L-RAT) puts forward the notion that disparities in individuals' daily activities and risk-taking behaviors render certain individuals more conducive targets for victimization (Algahtany et al., 2019; Finkelhor & Asdigian, 1996). Nonetheless, recent findings of Parti's study reveal that the frequency of social media use predicted online fraud victimization among younger individuals, with no such predictive relationship among older individuals (Parti, 2022). Additionally, the duration of time spent online did not prove to be a predictor of victimization. In contrast, the usage of smartphones, which can be indicative of an individual's online lifestyle, demonstrated its potential as both an indicator and predictor of online fraud.

Fraudsters often exploit cognitive biases or errors stemming from negative lifestyles in their attacks, eliciting automatic emotional responses from their victims (Emami et al., 2019). However, certain studies have indicated a positive predictive impact of negative life experiences (Alseadoon et al., 2013; Emami et al., 2019). Sur et al. (2021) indicated that experiencing negative life events did not have a significant connection with self-reported fraud victimization, introducing uncertainty about the role of this factor.

People's shopping habits vary significantly when it comes to device usage. Some individuals prefer shopping via mobile phones, while others opt for computers. However, there remains a gap in the research concerning these habits and their correlation with online fraud. It raises the question of whether mobile phone users are more susceptible to fraud compared to computer users. Although some studies have explored the role of the type of device, they often fail to establish links with personal factors and other relevant variables such as (Goel et al., 2012; Hao et al., 2023; Hernacki, 2011; Karo & Sebastian, 2019; Ponce et al., 2022; Sophia et al., 2023). In other words, while previous research may have examined the influence of device choice on online fraud vulnerability, it frequently omits the examination of how individual characteristics and various other factors interact with this choice. Investigating these interactions could provide a more comprehensive understanding of the relationship between device preference and susceptibility to online fraud which study will pave the way for groundbreaking research into individual habits regarding device usage and their intricate associations with various other factors, notably online fraud. By exploring the nuanced relationships between personal habits in device choice and susceptibility to online fraud, this research endeavors to establish a solid foundation for future investigations in this crucial and hitherto understudied domain. The findings from this study can serve as a springboard for in-depth explorations and a more comprehensive understanding of the interplay between device preferences, personal traits, and online fraud vulnerability. In terms of the association between income and fraud online, some studies have linked the individual's income to being vulnerable to direct personal attacks or attacks their property (Flexon et al., 2023; Kellner et al., 1996), but there is a very large shortage of studies that have investigated the relationship between income and online fraud (Mittal et al., 2006).

2.5 Theoretical Framework, Research Gaps and Future Directions

In summary, the findings discussed emphasize the significance of factors such as demographics, income, preferred shopping, trust tendency and following the advertisements in shaping victimity and their potential to forecast fraud victimization. However, as previously noted, previous research has produced inconsistent results. Therefore, this study aims to provide clarity on the role of these victimity features in the context of online fraud victimization in Saudi Arabia. Drawing from prior research, our hypothesis is that discernible differences exist between individuals who become victims and those who do not, particularly in terms of demographics, income, preferred shopping, trust tendency and following the advertisements. These factors are expected to be substantial predictors of online fraud.

3. Data and Study Methodology

The sample consisted of volunteers who completed online questionnaires from different areas of Saudi Arabia. The questionnaire was designed and distributed online. These questionnaires gathered information from the participants, including their demographic details, experience with online fraud, their preference for online or physical purchasing, their level of trust toward social application and suspicion messages, and susceptibility to promotional advertisements. All the returned questionnaires were filled out anonymously and voluntarily by the participants after obtaining their consent. In total, 723 valid questionnaires were collected. The participants included 487 males, constituting 67.4% of the sample, and 236 females, accounting for 32.6%. They were divided into five groups between 18 and 50 and above, as the questionnaire was designed not to accept respondents under 18. The average age was 45 years (with a standard deviation of 13.46).

In this study, we aim to investigate the influence of these factors on online fraud. To achieve this, we will compare individuals who have experienced online fraud with those who have not in order to create profiles of individuals with a high probability of being victims, thus identifying those at a higher risk of becoming victims of online fraud.

Among the participants, 515 individuals, or 71.5%, reported having experienced online fraud, while 208 individuals, or 28.4%, had not encountered online fraud victimization (Table 1).

Table 1: Case Processing Summary

Have you ever been defrauded financially through mobile or personal computer?	Valid N (listwise)
Positive	515
Negative	208

Larger values of the test result variable(s) indicate stronger evidence for a positive actual state.

a. The positive actual state is Yes.

Demographic variables, encompassing gender, age, marital status, education level, majors, type of job, income, preferred shopping, trust tendency to social media applications or suspicious messages, and following the advertisements along with participants' previous experiences with online fraud, formed the foundational information for this analysis. To evaluate participants' impulsiveness levels, the Barratt Impulse Scale (BIS-11) developed by Stanford et al. (1996) was employed. It is the most commonly used self-assessment tool for measuring impulsive personality traits. Eleven items were selected from the original scale, focusing on impulsiveness in both actions and planning. The scale utilized a 4-point scoring system, ranging from 1 (never) to 4 (always). Total scores on this scale could range from 8 to 24, with higher scores indicating a greater degree of impulsiveness in both actions and planning. Confirmatory factor analysis of this scale produced the following results of this equation: , root-mean-square error of approximation (RMSEA) = 0.05, comparative fit index (CFI) = 0.92, and Tucker-Lewis Index (TLI) = 0.93. In this study, the Cronbach's alpha coefficient for the scale was determined to be 0.61. Cronbach's alpha was chosen to assess internal consistency and data reliability, and it was satisfactory for completing the analysis process.

Trust tendency among participants was measured using the questionnaire on the deception tendency of the elderly, as compiled by Azizli et al. (2016). This questionnaire consists of 4 items, including questions like "How likely are you to receive help when seeking assistance from government agencies responsible for handling online fraud?" Responses are recorded using a 4-point scoring method, with 1 indicating "very unlikely" and 4 indicating "very likely." The total score can range from 10 to 40, with higher scores reflecting a greater trust tendency. The confirmatory factor analysis for this scale yielded the following results: , RMSEA = 0.05, CFI=0.93, and TLI= 0.89. The Cronbach's alpha coefficient for the scale was calculated to be 0.75.

To assess the participants' usage of devices, specifically their smartphones and personal computers, the Smartphone Addiction Usage Scale developed by (Kwon et al., 2013) was employed. His scale incorporated two items, for instance, "I frequently check my mobile to enter social media applications." Participants provided responses using a 5-point rating system, where 1 indicated "totally disagree," and 5 indicated "totally agree." The total score could range from 2 to 10, with higher scores reflecting a greater level of usage of one of the

two devices, either a smartphone or a personal computer. The results of the confirmatory factor analysis for this scale were as follows: , RMSEA =0.00, CFI = 1.00, and TLI =1.00, while Cronbach's alpha coefficient for the scale was determined to be 0.71.

To measure the effects of proclivity toward trust and susceptibility to the allure of promotional advertisements, the scale comprises 8 items, featuring statements such as "I encountered a negative online fraud incident in the past 12 months." Participants rated these items using a 3-point scale, with 0 indicating no occurrence, 1 denoting an occurrence without significant distress, and 2 representing severe distress. The total score can vary between 0 and 30, with higher scores indicating a more pronounced adverse impact and a heightened level of distress. The results of the confirmatory factor analysis for this scale produced the following: , RMSEA= 0.06, CFI = 0.94, and TLI = 0.87, while Cronbach's alpha coefficient for the scale was found to be 0.79.

Study analysis and results

A binomial logistic regression has been applied to predict the probability that an observation falls into these categories which are victim and non-victim of a dichotomous dependent variable based on demographic variables (age, education level, job, major, and income), a preference for online purchasing, a proclivity toward trust, the choice of device (be it a computer or smartphone), and susceptibility to the allure of promotional advertisements. To make sure that our study design will fit the analysis, linearity has been tested and natural log transformations have been created to check the new variables (victim and non-victim) are linearly related to the logit of the other factor. Percentage accuracy in classification (PAC) was 71.50 which is considered as a good sign for the model accuracy. Significant elements are gender, age, and advertisement while marital status, education, major, kind of job, income and preferred shopping aren't significant (Table 2).

Table 2:Logistic Regression Predicting Likelihood of online fraud victimization

		B	S.E.	Wald	df	p	Odds ratio	95% C.I.for Odds ratio	
								Lower	Upper
Step 1[a]	Gender	-.526	.215	5.960	1	.015	.591	.388	.902
	Age	.235	.073	10.420	1	.001	1.265	1.097	1.459
	Marital status	.204	.184	1.233	1	.267	1.227	.855	1.759
	Education	.089	.073	1.499	1	.221	1.093	.948	1.261
	Majors	-.083	.082	1.015	1	.314	.921	.784	1.081
	Type of job	.094	.123	.585	1	.444	1.098	.863	1.398
	Income	-.087	.115	.571	1	.450	.917	.731	1.149
	Prefer purchasing	.014	.078	.031	1	.861	1.014	.870	1.181
	Following advertisement	.200	.085	5.550	1	.018	1.221	1.034	1.442
	Constant	-2.206	.846	6.804	1	.009	.110		

a. Variables: gender, age, marital status, education, majors, type of job, income, preferred purchasing, allure of promotional advertisements.

To correctly classify cases, the ROC curve has been applied to the data. The ROC model refers to its capacity to differentiate between participants who experience online fraud and those who do not. In essence, it involves the model's ability to predict which individuals are likely to have or not have experienced online fraud (Figure 1). The ROC curve's area was 0.857 (95% CI, 0.614 to 0.801), indicating a high level of discrimination as classified by Hosmer Jr et al. (2013) (Table 3).

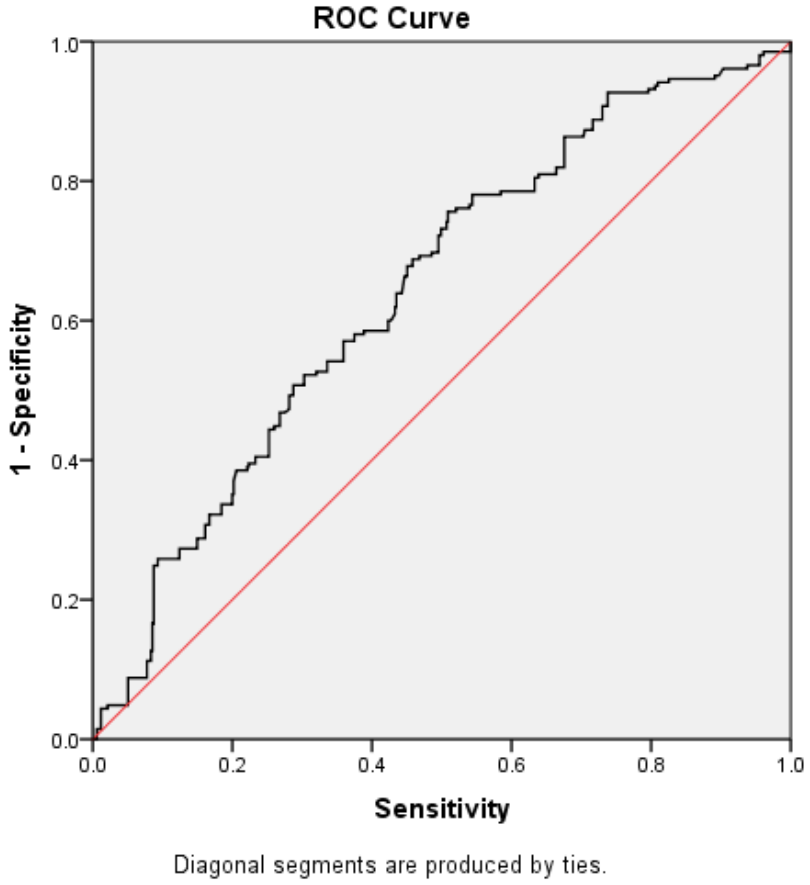

Figure 1: ROC Curve

Table 3: ROC test result

Area Under the Curve				
Test Result Variable(s): Predicted probability				
			Asymptotic 95% Confidence Interval	
Area	Std. Error	Asymptotic Sig.b	Lower Bound	Upper Bound
.857	.022	.000	.614	.801
The test result variable(s): Predicted probability has at least one tie between the positive actual state group and the negative actual state group.				
a. Under the nonparametric assumption b. Null hypothesis: true area = 0.5				

Demographic characteristics, susceptibility to promotional advertisements, trust tendency, and device usage were reported in descriptive statistics. Differences in demographic attributes between individuals vulnerable to fraud and those not were examined through chi-square tests and independent sample t-tests. An independent sample t-test was applied to evaluate variations in technology usage between the two groups. Binary logistic regression analyses were employed to understand how these variables collectively predicted instances of online fraud. Data analysis was performed using Statistical Product and Service Solutions (SPSS) version 23.0, with statistical significance established at $p < 0.05$.

Table 4 outlines the demographic characteristics of the sample, categorizing it into two groups: individuals vulnerable to fraud and those not. Among non-victims, the average age stood at 38.43 (with a standard deviation of 12.84), while victims had an average age of 32.66 (with a standard deviation of 9.75). The gender distribution revealed 55.8% men among non-victims and 46.2% among victims. For educational background, 20.2% of non-victims had completed high school or its equivalent, whereas the corresponding figure for victims was 48.6%. To compare non-victims and victims, an independent sample t-test was performed for age, while a chi-square test was applied for gender and education. The results in Table 1 indicate significant disparities between the two groups concerning age and education. Victims tended to be between 22 and 50 years old and had lower educational attainment than non-victims, which aligns with our initial hypothesis. Moreover, gender was identified as a significant factor in this study, further supporting the hypothesis. The noteworthy finding here is that individuals with completely non-educated appear to be less affected by online fraud, which contradicts our initial hypothesis (Table 4).

Table 4:The demographic characteristics of online fraud victims and non-victim

Test variables	Non- online fraud victims	Online fraud victims	t or x^2
	M (SD) or n (%)	M (SD) or n (%)	
Age	38.43 (12.84)	32.66 (9.75)	10.83***
Gender			-0.56
Male	(55.8)	(46.2)	
Female	(49.3)	(51.0)	
Education			-7.21***
Non-educated	(18.3)	(1.0)	
High school	(20.2)	(48.6)	
Diploma	(49.5)	(41.3)	
Bachelor	(32.3)	(28.2)	
Masters	(29.3)	(26.7)	
Ph.D	(5.4)	(1.0)	
***p < 0.001.			

Table 5 presents the mean scores (M) and standard deviations (SD) for susceptibility to promotional advertisements and highlights the differences between the two groups: those who have fallen victim to online fraud and those who have not. The distinctions were identified using independent sample t-tests. The results indicate significant variations between these groups regarding susceptibility to promotional advertisements, trust tendencies, and device usage. Victims displayed considerably higher levels of susceptibility to promotional advertisements, trust tendencies, and device usage when compared to non-victims.

Table 5: Differences between victims and non-victims in influenced by the various variables.

Factors	Victims	SD	t	p
influenced by advertisements	No	18.45 (3.75)	−7.32	<0.001
	Yes	20.28 (3.46)		
Devices usage	No	19.12 (4.28)	−7.83	<0.001
	Yes	21.22 (4.77)		
Trust tendency toward to applications	No	8.93 (3.36)	−2.42	0.034
	Yes	11.16 (3.56)		

To analyze the predictive effects of age, education level, income, a proclivity toward trust, and susceptibility to the allure of promotional advertisements on online fraud victimization, binary logistic regression was applied with those who have been victims as the dependent variable. These variables were age, gender, education, trust tendency, and devices usage. The independent variables were victims and non-victims. As shown in (Table 6), age, education level, income, and the choice of device (be it a computer or smartphone) have significant positive predictive effects on online fraud.

Table 6: Predictors of online fraud victimization.

Factors	B	(B) (95% CI)
Age	−0.07***	0.93 (0.92–0.95)
Gender	0.13**	1.14 (0.85–1.52)
Education	-0.42***	0.66 (0.60–0.73)
Income	-0.08***	
Allure of promotional advertisements	0.06*	1.06 (1.01–1.11)
Proclivity toward trust	0.05**	1.05 (1.02–1.09)
Devices usage	-0.06***	1.00 (0.96–1.05)
*p < 0.05, **p < 0.01, ***p < 0.001.		

4. Discussion

In this research, it was observed that as age increases, the likelihood of falling victim to online fraud also increases. However, the existing literature presents varying results when it comes to age as a protective or predictive factor in online fraud victimization. Some studies, like Fan and Yu (2022), align with our findings by suggesting that older individuals are more susceptible to fraud. In contrast, other studies, such as Parti (2022), argue that younger people are at higher risk of online fraud. Meanwhile, there are studies, like Whitty (2020), that have found age to be unrelated to cyber scam victimization. This variability indicates that age alone may not be a consistent predictor of online fraud. Instead, various factors, both demographic and otherwise, play a more significant role, as explored in our study.

Preventing victimization effectively relies heavily on exploring factors that contribute to individuals becoming victims. In this study, we examined the correlation between demographic variables (gender, age, marital status, education, majors, type of job, income), the allure of promotional advertisements, type of device used, and preference for online purchasing. Univariate analyses revealed notable differences in age, education, trust tendency, and device usage. These findings generally aligned with our hypotheses, except for the null effect observed in gender. Logistic regression analysis identified age, education, and trust tendency as significant predictive factors for victimization.

The independent sample t-test indicates that individuals who fall prey to fraud are considerably younger and possess lower education levels compared to those who do not become victims. Additionally, the logistic regression analysis points to a detrimental predictive impact of these two demographic factors. These findings are in alignment with our initial hypothesis, which posits that a lower age and educational attainment correlate with an increased likelihood of becoming a victim of fraud. In Saudi Arabia, a developing country where technologies play an increasingly dominant role in our lives (Aljeaid et al., 2020), it is crucial to ensure that individuals are well-informed about security risks, a realization that often becomes more pronounced after experiencing privacy violations.

Aljeaid et al. (2020) conducted an experiment to assess the assumption that end users in Saudi Arabia lack sufficient knowledge and skills to protect themselves from cyberattacks. The results revealed that 77% of the participants became victims of such attacks, with a higher prevalence among students. Interestingly, occupation was found to be uncorrelated with the likelihood of exposure to a phishing attack which supported our hypothesis and finding. So, we found that the major is not a significant factor in online fraud. These findings underscore the necessity of enhancing cybersecurity knowledge and highlight the importance of cybersecurity awareness programs.

Exploring the connection between the use of different devices (smartphone or personal computer) and online fraud. The findings indicate that while device usage is not a significant predictor of online fraud, there is a positive correlation with victimization. In line with lifestyle exposure theory, individuals with varying lifestyles, such as spending extended periods on different websites, may encounter different levels of crime risks. If certain lifestyles involve more exposure to potential risks (such as fraud websites) or frequent situations conducive to fraud, the risk of victimization tends to be higher (Choi et al., 2019).

Our research indicates that the variable (Major) is correlated with awareness of the internet and online scams. Elevated levels of self-assuredness in computer use, internet proficiency, and knowledge of security measures are linked with a reduced likelihood of falling prey to phishing schemes (Wright & Marett, 2010). Nonetheless, an excess of confidence in individuals with higher education might elevate their chances of being scammed (Parti, 2022). Our findings corroborate the theory that gender is an indicator of scam victimization. The study reveals a distinction in gender between those who have been scammed and those who have not. These outcomes are in line with Whitty's (2020) research, which found a greater tendency for women to be duped by consumer scams, whereas men were more prone to fall for investment scams. The influence of gender seems to be significant in relation to specific scam types. Subsequent studies could investigate the demographic factors linked with various forms of online fraud in Saudi Arabia to develop a more comprehensive understanding and create targeted prevention measures.

Our research suggests that impulsiveness and a tendency to trust play significant roles in predicting susceptibility to fraud. We

have found that individuals who display higher levels of impulsiveness and a natural inclination to trust others are at an increased risk of becoming victims of fraud. Defined as the propensity to react swiftly to unexpected stimuli, impulsiveness can have negative repercussions due to insufficient consideration of the outcomes of one's actions (Algahtany & Kumar, 2016; Strickland & Johnson, 2021) People who are impulsive are often more easily swayed by others and tend to place their trust in swindlers, particularly in complex fraudulent schemes. Similarly, a natural tendency to trust, which refers to a person's baseline level of trust in others without detailed knowledge about them, is linked to a greater likelihood of falling prey to fraud. It has been observed that those who fall victim to online fraud typically have a higher trust level in others (Algahtany et al., 2022; Grazioli & Jarvenpaa, 2000; Van Wilsem, 2013). Those who inherently trust others are more prone to being misled, especially in scenarios involving communication and internet-based fraud, where they may not have enough contextual information to make informed judgments (Algahtany et al., 2018; Norris et al., 2019; Wang & Topalli, 2022).

Our research explores the connection between the use of devices like smartphones and personal computers and the incidence of online fraud victimization. We focused on assessing how the use of these devices impacts susceptibility to online scams. While the specific type of device used is not a direct indicator of online fraud likelihood, there is a positive correlation with victimization. In line with the lifestyle exposure theory, we recognize that individuals with different lifestyle patterns face varying levels of criminal risk. Particularly, those who frequently use devices for online activities may have a heightened risk of encountering online fraud. Our findings indicate that smartphone users are more susceptible to online fraud than those who predominantly use personal computers for financial transactions. Additionally, giving money to scammers can increase the likelihood of being targeted again. The reliance on smartphones, which often denotes a lifestyle abundant in online activities, escalates the risk of encountering online scams, making users more attractive targets for fraudsters. For future studies, more detailed inquiries could shed light on how specific device usage, especially in the context of online activities, influences the risk of online fraud. The findings highlight the need for pertinent departments to focus on and introduce specific educational programs aimed at preventing online fraud.

Experiencing negative life events has been identified as a contributing factor to online fraud vulnerability (Algahtany et al., 2016; Algahtany et al., 2014; Anderson, 2019; Deliema et al., 2020; Emami et al., 2019). Our study supports the theory that adverse habits are predictors of becoming a fraud victim. This correlation can be explained in several ways. First, negative life events may increase susceptibility to fraud by diminishing social support and reducing participation in external social activities, leading to increased internet use (Sur et al., 2021). Second, those undergoing difficult experiences, such as divorce or job loss, might seek more connections, job opportunities, or financial assistance online, thus encountering more scam attempts. A third explanation is based on the Elaboration Likelihood Model (ELM)(Petty et al., 1986), suggesting that individual mood variations at the time of message reception influence the intensity of processing a potential scam communication (Norris & Brookes, 2021). In our study, the impact of negative life events might be mediated by how a negative mood affects the processing of scam messages. Future studies should explore how various negative life events influence susceptibility to different types of online fraud.

5. Conclusion

In conclusion, this research has comprehensively examined the multifaceted aspects influencing online fraud victimization, revealing a complex interplay of demographic,

psychological, technological, and lifestyle factors. The study underscores the increased vulnerability to online fraud with advancing age, contradicting some existing literature while supporting others, highlighting the nuanced role of age in online scam susceptibility. Our investigation into demographic variables such as gender, age, marital status, education, and income, along with factors like device usage and online purchasing preferences, reveals that age, education, and trust tendencies are significant predictors of fraud victimization.

Notably, the study finds a positive correlation between device usage, particularly smartphones, and fraud victimization, suggesting that lifestyle habits, including prolonged online activities, elevate the risk of encountering online scams. This aligns with the lifestyle exposure theory, which posits that certain lifestyle choices increase exposure to potential risks. The research also emphasizes the role of psychological traits such as impulsiveness and trust tendency in increasing susceptibility to fraud, with impulsive individuals and those with a higher inherent trust level being more prone to deception.

Moreover, the impact of negative life events on fraud vulnerability is highlighted, suggesting that such experiences may lead to increased internet use and greater exposure to scams. The Elaboration Likelihood Model (ELM) further elucidates how individual mood variations at the time of message reception can affect the processing of scam communications.

The findings of this study advocate for the implementation of targeted educational programs to enhance awareness and prevention of online fraud. It is imperative for relevant authorities and institutions, especially in technologically evolving contexts like Saudi Arabia, to focus on educating the public about the risks associated with online activities and cyberattacks. Future research should delve deeper into exploring the specific roles of various negative life events and device usage patterns in different types of online fraud, thereby aiding in the development of more nuanced and effective prevention strategies. In essence, this research contributes significantly to the understanding of online fraud victimization, offering valuable insights for future initiatives aimed at reducing the prevalence of such crimes.

This study will pave the way for groundbreaking research in the field of online fraud and device usage. By delving into the complex associations between personal habits related to device choice and their connection to online fraud vulnerability, this research has the potential to set the stage for future pioneering investigations. The findings from this study can act as a catalyst, igniting further in-depth explorations and a deeper understanding of the intricate interplay between device preferences, individual characteristics, and susceptibility to online fraud.

Limitations and Future Research

Considering the myriad of fraud techniques globally and the diverse needs and characteristics of individuals, it's plausible that various types of individuals are prone to falling for different scams. This analysis might have gained more insight by delving into the risk factors specific to each fraud type. One of the limitations of this study is the lack of representativeness and broad applicability due to the sampling technique used. Future studies should focus on implementing more relevant sampling strategies and enlarging the sample base. Moreover, this study's reliance on self-reporting can introduce biases influenced by how respondents interpret questions, perceive their actions, and conform to social norms. Additionally, a minor segment of participants who are unaware of being fraud victims might have been inaccurately categorized in the survey, potentially impacting the findings. Future research should explore experimental or behavioral methodologies to more thoroughly examine the risk factors

associated with fraud victimization and the mechanisms behind these risks, in order to gather more objective and reliable data.

Declaration of competing interest

The authors affirm that the conduct of this research was free from any commercial or financial affiliations that might be perceived as a conflict of interest.

Declaration of generative AI in scientific writing

The authors affirm that the conduct of this research was free from using generative AI in any part of this research.

6. References

Alanezi, F. (2016). Perceptions of online fraud and the impact on the countermeasures for the control of online fraud in Saudi Arabian financial institutions Brunel University London].

Alanezi, F., & Brooks, L. (2014). Combatting online fraud in Saudi Arabia using general deterrence theory (GDT).

Alfuraih, S. (2008). E-commerce and e-commerce fraud in Saudi Arabia: A case study. 2008 International Conference on Information Security and Assurance (isa 2008),

Algahtany, M., & Kumar, L. (2016). A method for exploring the link between urban area expansion over time and the opportunity for crime in Saudi Arabia. Remote Sensing, 8(10), 863.

Algahtany, M., Kumar, L., & Barclay, E. (2019). The impact of road networks on crime rates in Saudi Arabia.

Algahtany, M., Kumar, L., & Barclay, E. (2022). A tested method for assessing and predicting weather-crime associations. Environmental Science and Pollution Research, 29(49), 75013-75030.

Algahtany, M., Kumar, L., Barclay, E., & Khormi, H. M. (2018). The spatial distribution of crime and population density in Saudi Arabia. Crime prevention and community safety, 20, 30-46.

Algahtany, M., Kumar, L., & Khormi, H. (2016). Are immigrants more likely to be involved in criminal activity in Saudi Arabia? Open Journal of Social Sciences, 4(03), 170.

Algahtany, M., Kumar, L., & Khormi, H. M. (2014). Spatio-temporal changes on crime patterns in Saudi Arabia from 2003–2012. Journal of Law and Social Sciences, 4, 11-19.

Alghamdi, F. S., & Nor, R. M. (2023). Evaluating E-Commerce Engagement Factors In Saudi Arabia: Financial Loss, Identity Theft And Privacy Policies. International Journal of Professional Business Review: Int. J. Prof. Bus. Rev., 8(12), 4.

Aljeaid, D., Alzhrani, A., Alrougi, M., & Almalki, O. (2020). Assessment of end-user susceptibility to cybersecurity threats in Saudi Arabia by simulating phishing attacks. Information, 11(12), 547.

Alonazi, W. B. (2020). Fraud and Abuse in the Saudi healthcare system: a triangulation analysis. INQUIRY: The Journal of Health Care Organization, Provision, and Financing, 57, 0046958020954624.

Alseadoon, I. M., Othman, M. F. I., Foo, E., & Chan, T. (2013). Typology of phishing email victims based on their behavioural response.

Anderson, K. B. (2019). Mass-market consumer fraud in the United States: A 2017 update. Federal Trade Commission. Washington, DC.

Azizli, N., Atkinson, B. E., Baughman, H. M., Chin, K., Vernon, P. A., Harris, E., & Veselka, L. (2016). Lies and crimes: Dark Triad, misconduct, and high-stakes deception. Personality and individual differences, 89, 34-39.

Balleisen, E. J. (2018). The" Sucker List" and the Evolution of American Business Fraud. Social Research: An International Quarterly, 85(4), 699-726.

Bossler, A. M., & Holt, T. J. (2010). The effect of self-control on victimization in the cyberworld. Journal of Criminal Justice, 38(3), 227-236.

Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. Security Journal, 27, 36-54.

Carter, N., & Weber, J. (2010). Not Pollyannas: Higher generalized trust predicts lie detection ability. Social Psychological and Personality Science, 1 (3), 274–279. In.

Choi, K.-S., Cho, S., & Lee, J. R. (2019). Impacts of online risky behaviors and cybersecurity management on cyberbullying and traditional bullying victimization among Korean youth: Application of cyber-routine activities theory with latent class analysis. Computers in Human Behavior, 100, 1-10.

Deliema, M., Shadel, D., & Pak, K. (2020). Profiling victims of investment fraud: Mindsets and risky behaviors. Journal of Consumer Research, 46(5), 904-914.

Emami, C., Smith, R. G., & Jorna, P. (2019). Online fraud victimisation in Australia: Risks and protective factors. Australian Institute of Criminology.

Fan, J. X., & Yu, Z. (2022). Prevalence and risk factors of consumer financial fraud in China. Journal of family and economic issues, 43(2), 384-396.

Finkelhor, D., & Asdigian, N. L. (1996). Risk factors for youth victimization: Beyond a lifestyles/ routine activities theory approach. Violence and victims, 11(1), 3.

Flexon, J. L., Liu, L., Greenleaf, R. G., & James, N. (2023). Income and Calling the Police: Examining a Nuanced Relationship Toward Theoretical Refinement. Victims & Offenders, 1-22.

Goel, A., Tyagi, A., & Agarwal, A. (2012). Smartphone forensic investigation process model. International Journal of Computer Science & Security (IJCSS), 6(5), 322-341.

Grazioli, S., & Jarvenpaa, S. L. (2000). Perils of Internet fraud: An empirical investigation of deception and trust with experienced Internet consumers. IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 30(4), 395-410.

Han, D., Pang, Z., He, L., Zhou, X., & Zhang, S. (2023). Management response and user idea generation: evidence from an online open innovation community. Information Technology and Management, 24(4), 381-400.

Hao, J., Hao, X., Tian, Z., Wang, Y., & Zheng, D. (2023). Effects of service attributes and competition on electronic word of mouth: an elaboration likelihood perspective. Information Technology and Management, 1-13.

Hernacki, A. T. (2011). A Vague Law in a Smartphone World: Limiting the Scope of Unauthorized Access Under the Computer Fraud and Abuse Act. Am. UL Rev., 61, 1543.

Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2008). Low self-control, routine activities, and fraud victimization. Criminology, 46(1), 189-220.

Hosmer Jr, D. W., Lemeshow, S., & Sturdivant, R. X. (2013). Applied logistic regression (Vol. 398). John Wiley & Sons.

Judges, R. A., Gallant, S. N., Yang, L., & Lee, K. (2017). The role of cognition, personality, and trust in fraud victimization in older adults. Frontiers in psychology, 8, 588.

Kadoya, Y., Khan, M. S. R., Narumoto, J., & Watanabe, S. (2021). Who is next? A study on victims of financial fraud in Japan. Frontiers in psychology, 12, 649565.

Karo, R. K., & Sebastian, A. (2019). Juridical analysis on the criminal act of online shop fraud in Indonesia. Lentera Hukum, 6, 1.

Kellner, F., Webster, I., & Chanteloup, F. (1996). Describing and predicting alcohol use-related harm: an analysis of the Yukon Alcohol and Drug Survey. Substance use & misuse, 31(11-12), 1619-1638.

Kwon, M., Kim, D.-J., Cho, H., & Yang, S. (2013). The smartphone addiction scale: development and validation of a short version for adolescents. PLoS one, 8(12), e83558.

Lang, F., & Riegel, L. (2023). Acceptance of online customer channels for damage claims in Germany. Information Technology and Management, 1-16.

Lee, C. S. (2021). Online fraud victimization in China: A case study of Baidu Tieba. Victims & Offenders, 16(3), 343-362.

Li, F. (2023). Network Security Evaluation and Optimal Active Defense based on Attack and Defense Game Model. 2023 International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE),

Mendelsohn, B. (1963). The origin of the doctrine of victimology. Exerpta Criminologica, 3, 239-245.

Mesch, G. S., & Dodel, M. (2018). Low self-control, information disclosure, and the risk of online fraud. American Behavioral Scientist, 62(10), 1356-1371.

Mikkola, M., Oksanen, A., Kaakinen, M., Miller, B. L., Savolainen, I., Sirola, A., Zych, I., & Paek, H.-J. (2020). Situational and individual risk factors for cybercrime victimization in a cross-national context. International journal of offender therapy and comparative criminology, 0306624X20981041.

Mittal, S., Gupta, R., Mohania, M., Gupta, S. K., Iwaihara, M., & Dillon, T. (2006). Detecting frauds in online advertising systems. International Conference on Electronic Commerce and Web Technologies,

Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. International Journal of Cyber Criminology, 5(1), 773.

Ni, P., & Wang, Q. (2022). Internet and Telecommunication Fraud Prevention Analysis based on Deep Learning. Applied Artificial Intelligence, 36(1), 2137630.

Norris, G., & Brookes, A. (2021). Personality, emotion and individual differences in response to online fraud. Personality and individual differences, 169, 109847.

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

Parti, K. (2022). "Elder Scam" Risk Profiles: Individual and Situational Factors of Younger and Older Age Groups' Fraud Victimization.

Pattinson, M. R., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. A. (2011). Managing Phishing Emails: A Scenario-Based Experiment. HAISA,

Petty, R. E., Cacioppo, J. T., Petty, R. E., & Cacioppo, J. T. (1986). The elaboration likelihood model of persuasion. Springer.

Ponce, E. K., Sanchez, K. E., & Andrade-Arenas, L. (2022). Implementation of a web system: Prevent fraud cases in electronic transactions. International Journal of Advanced Computer Science and Applications, 13(6).

Pratt, T. C., Turanovic, J. J., Fox, K. A., & Wright, K. A. (2014). Self-control and victimization: A meta-analysis. Criminology, 52(1), 87-116.

Pyrkh, M. (2023). FRAUD PREVENTION TECHNIQUES FOR E-COMMERCE MERCHANTS, USING PAYMENT TRANSACTION RISK SCORES.

Reisig, M. D., & Holtfreter, K. (2013). Shopping fraud victimization among the elderly. Journal of Financial Crime, 20(3), 324-337.

Reyns, B. W., & Randa, R. (2020). No honor among thieves: Personal and peer deviance as explanations of online identity fraud victimization. Security Journal, 33, 228-243.

Ross, M., Grossmann, I., & Schryer, E. (2014). Contrary to psychological and popular opinion, there is no compelling evidence that older adults are disproportionately victimized by consumer fraud. Perspectives on Psychological Science, 9(4), 427-442.

Shannon, H. S., Robson, L. S., & Guastello, S. J. (1999). Methodological criteria for evaluating occupational safety intervention research. Safety Science, 31(2), 161-179.

Sophia, I. J., Meganathan, R., Dhanasakkaravarthi, B., Kumar, S. S., & Mishra, A. (2023). Accurate Click Fraud Rapid Detection of AD Requests for Smartphone Platforms. 2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC),

Stanford, M. S., Greve, K. W., Boudreaux, J. K., Mathias, C. W., & Brumbelow, J. L. (1996). Impulsiveness and risk-taking behavior: Comparison of high-school and college students using the Barratt Impulsiveness Scale. Personality and individual differences, 21(6), 1073-1075.

Strickland, J. C., & Johnson, M. W. (2021). Rejecting impulsivity as a psychological construct: A theoretical, empirical, and sociocultural argument. Psychological review, 128(2), 336.

Sule, B., Sambo, U., & Yusuf, M. (2022). Countering cybercrimes as the strategy of enhancing sustainable digital economy in Nigeria. Journal of Financial Crime.

Sur, A., DeLiema, M., & Brown, E. (2021). Contextual and social predictors of scam susceptibility and fraud victimization. Available at SSRN 4053903.

Van Belle, R., Baesens, B., & De Weerdt, J. (2023). CATCHM: A novel network-based credit card fraud detection method using node representation learning. Decision Support Systems, 164, 113866.

Van Wilsem, J. (2013). 'Bought it, but never got it'assessing risk factors for online consumer fraud victimization. European sociological review, 29(2), 168-178.

Vishwanath, A. (2015). Examining the distinct antecedents of e-mail habits and its influence on the outcomes of a phishing attack. Journal of Computer-Mediated Communication, 20(5), 570-584.

Wang, F., & Topalli, V. (2022). Understanding Romance Scammers Through the Lens of Their Victims: Qualitative Modeling of Risk and Protective Factors in the Online Context. American Journal of Criminal Justice, 1-37.

Whitty, M. T. (2020). Is there a scam for everyone? Psychologically profiling cyberscam victims. European Journal on Criminal Policy and Research, 26(3), 399-409.

Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. Computers in Human Behavior, 72, 412-421.

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