Scientific Research Publishing

Open Journal of Business and Management, 2024, 12, 2949-2964
https://www.scirp.org/journal/ojbm
ISSN Online: 2329-3292
ISSN Print: 2329-3284

The Interplay of Social Behaviour and Demographics in Cyber Scam Susceptibility: A Singapore Study

Johan H. M. Buse[1*], Christopher Fong[2], Shilpi Tripathi[3*]

[1]Department of Psychology, London Metropolitan University, London, United Kingdom
[2]Department of Psychology, University of Roehampton, London, United Kingdom
[3]Singapore City, Singapore
Email: *Johanbuse@gmail.com, *tripathi888@gmail.com

How to cite this paper: Buse, J. H. M., Fong, C., & Tripathi, S. (2024). The Interplay of Social Behaviour and Demographics in Cyber Scam Susceptibility: A Singapore Study. *Open Journal of Business and Management, 12,* 2949-2964.
https://doi.org/10.4236/ojbm.2024.125151

Received: January 24, 2024
Accepted: August 17, 2024
Published: August 20, 2024

Abstract

Cyber scams, a subset of cybercrimes, have increased globally, posing significant threats to individuals and communities. These scams often result in financial and psychological damages. Cyber scams are fraudulent activities conducted online, leading to financial loss and emotional distress for victims. Common types include phishing (fraudulent emails seeking personal information), identity theft, online shopping scams, investment scams, romance scams, and tech support scams. Impacts range from direct financial losses, psychological trauma, and identity theft consequences, to broader social implications like erosion of trust in digital platforms. Prevention involves awareness, secure online practices, regular monitoring of accounts, verification of information sources, and prompt reporting of suspicious activities. Previous research has indicated mixed results concerning demographic factors influencing scam susceptibility. This study aims to comprehensively analyze these factors, including age, gender, education level, marital status, employment status, income level, financial situation, ethnicity, addiction, and social engagement. **Methodology:** The study employed a quantitative approach, administering a structured questionnaire to 300 participants, comprising both Singapore residents and non-residents. The methodology focused on Pearson's chi-square and Spearman's correlation tests to analyze the relationships between demographic factors, social engagement, and scam victimization. **Results:** The study's findings indicate a significant correlation between gender and scam victimization, with males showing higher susceptibility to investment-related scams. However, other demographic factors did not show a significant correlation with scam victimization. Additionally, the research found that social engagement does not significantly correlate with scam vic-

timization, challenging previously held notions. **Conclusion:** This research contributes to understanding cyber scam victimization by highlighting the importance of demographic factors and social engagement. It underscores the need for multifaceted approaches in prevention and intervention strategies tailored to address the specific risks faced by different demographic groups. The study's focus on Singapore limits its generalizability. Future research should explore these patterns in different cultural and geographical contexts and consider other variables like technological savviness and specific online behaviors.

Keywords

Cyber Scams, Psychological Impact, Singapore, Gender Differences, Investment Scams, Self-Acceptance, Wellbeing, Digital Fraud

1. Introduction

The rapid advancements in high-speed internet connectivity, including wired and wireless options, have revolutionized numerous facets of daily life. This technological evolution, mainly through devices like laptops, tablets, and smartphones, has enabled people to engage in various activities such as digital communication, online banking, e-commerce, real-time news, and virtual entertainment (Bossler & Berenblum, 2019). *Cybercrime* is a broad term that covers a wide range of computer-assisted criminal activities where technology plays a central role in facilitating communication but without direct physical interaction between the perpetrator and the victim (Algharabat et al., 2020). These crimes typically involve using computers and other digital technologies as critical tools or targets. This category includes crimes like unauthorized access to systems or networks, often called hacking (Mekler, 2022). It involves illegally entering digital spaces, breaching security protocols, or accessing confidential information without permission. This group covers identity theft, online fraud, and digital piracy (Buse et al., 2023). In the digital age, the rise of cyber scams has become a global concern, posing significant threats to individuals and communities (Cole, 2022). As technology becomes increasingly integrated into daily life, the avenues for cybercriminals to exploit vulnerabilities have expanded, making it imperative to understand factors contributing to an individual's susceptibility to these scams (Lubben et al., 2015). This study aims to delve into this crucial area by examining the correlation between various demographic factors and the likelihood of an individual becoming a victim of cyber scams. Additionally, it explores the potential link between social engagement and scam victimization (Ajayi, 2022).

Cyber scams, including a range of fraudulent online activities, have shown a worrying increase in both frequency and sophistication. These scams often result in financial losses and psychological impacts on victims (Bossler & Berenblum,

2019). The most direct impact is the loss of money. Victims can lose substantial amounts of money to these scams, sometimes their life savings. Falling victim to a scam can be emotionally distressing, leading to anxiety, depression, and a sense of betrayal. It can also lead to a loss of trust in online systems and transactions. Understanding the demographic characteristics that might influence an individual's vulnerability to such scams is essential for developing effective prevention strategies. Previous research has identified several factors, such as age, gender, education level, and income, as potential influencers of scam susceptibility (Maimon et al., 2019). However, results have been mixed, and there needs to be more consensus on which factors are most significant, especially in different cultural and geographical contexts, because Singapore's multicultural population is making the workplace diverse, with FTs and migrant workers from across the globe (Fong & Tripathi, 2021).

The demographic factors included in this study are gender, age, education level, marital status, living alone, employment status, income level, financial situation, ethnicity, and addiction (Cheng et al., 2020). As indicated by existing literature, these factors were chosen based on their potential relevance to cyber scam risks. For instance, age and education level have been hypothesized to influence an individual's ability to recognize and avoid online scams (Carter, 2020). Similarly, factors like income level and financial situation could impact the likelihood of being targeted by scammers and an individual's ability to recover from financial losses incurred due to scams (Burton et al., 2022).

In addition to these demographic factors, the study also investigates the role of social engagement in scam victimization. Social engagement refers to the extent and nature of an individual's interactions with their social network, including offline and online interactions (De Kimpe et al., 2021). It is hypothesized that higher levels of social engagement could provide individuals better access to information and support, potentially reducing their risk of falling victim to scams. Conversely, lower levels of social engagement might increase vulnerability due to isolation and a lack of access to information or support networks (Cole, 2022).

This study focuses on a sample from Singapore, with a comparative analysis involving a smaller group of non-Singapore residents. Singapore presents an interesting case study due to its high internet penetration rate and diverse, tech-savvy population. By including a sample of non-residents, the study aims to explore whether the observed patterns hold across different cultural and geographical contexts, thereby adding to the generalizability of the findings.

By addressing these research questions and gaps, the study aims to contribute significantly to understanding factors influencing susceptibility to cyber scams. It provides a nuanced perspective on how demographic variables and social engagement relate to scam victimization, offering valuable insights for targeted prevention and intervention strategies. The remaining of the study is structured as follows.

2. Research Design and Methodology

A mixed methods research design was used to investigate the impact and effects of cyber scams on Singapore residents. The rationale for opting for a mixed design research was the ability to provide a more detailed and deeper understanding of the effects and impacts of scams. Both the quantitative research and the qualitative research were conducted between 15 December 2022 and 15 March 2023. The quantitative study aimed to discover possible correlations between various demographic variables, social engagement, scam vulnerability, types of scams, self-acceptance, and well-being and being a scam victim. Three hundred and two respondents participated in the survey. Two respondents who failed to complete the consent form were subsequently excluded from the study, and 300 completed responses were accepted and analyzed as part of this study. With survey forms available in Mandarin and English, the quantitative research was 12 conducted online using Google Forms. Participation was anonymous. There are four official languages in Singapore. English is the language used for lecturing, while the student's official mother tongue is the second language taught. Based on 2020 census data (Census of Population, 2020), English is the language most spoken at home (48.3%) followed by Mandarin (29.9%). With English and Mandarin being spoken by 78.2% of the Singaporean population, offering the survey forms in English and Mandarin ensured that most Singaporeans could be addressed. The survey was not available in Malay and Tamil, the two other official languages of Singapore.

3. Recruitment of Candidates

Candidates were recruited via various online and social media channels and platforms, such as Facebook, Workplace, and WhatsApp, as well as online marketplaces, such as Carousel. A specific residency-related question was asked as part of the survey to ensure the ability to analyze data related to Singapore residents. Materials: The quantitative survey comprised 57 questions, which were structured into six sections to enable a study of correlations relating to well-being, social engagement, scam vulnerability, self-acceptance, and Singapore-based scam victims (**Table 1**). The survey length was considered and reflected upon, and there were concerns about the required time for the participants to complete the survey and the participants' possible reluctance to complete this longer and personal survey. Ultimately, obtaining a richer dataset was prioritized over the risk of the participants' reluctance to participate owing to the survey length.

4. Ethical Considerations and the Importance of Anonymity

Ethical considerations are an important aspect of research. For this quantitative research, a consent form was part of the survey. The participants were required to mandatorily sign the consent form to agree to the use of their data in the study. Owing to the nature of the topic under investigation, the anonymous data

treatment was considered important and necessary. Being scammed is a taboo subject. Many scam victims do not report scams because they feel ashamed or because of fear or the hassle involved. The surveys were completed using Google Forms. The participants could complete the study at their own time and convenience. No email or other personal data were requested. To minimize the risk of social desirability bias the questionnaire was constructed anonymously.

5. Sample Size Calculations

Cochran's formula was used to determine sample sizes needed for a confidence level of 95%, with a standard error of 5%. Two proportions were examined: 0.690 and 0.500. The initial sample sizes calculated were 329 for a population proportion of 0.690 and 385 for a population proportion of 0.500. Adjustments for the finite population sizes did not significantly alter the required sample sizes due to the large size of the populations considered. The results underscore the robustness of Cochran's formula in situations involving large populations. In this instance, the minimal impact of the finite population correction is consistent with other studies indicating that such corrections are often negligible for large populations (Johnson & Leone, 2005).

6. Instruments

The survey aimed to explore correlations related to well-being, social engagement, scam vulnerability, self-acceptance, and scam victims in Singapore. Data were collected through a structured questionnaire, distributed online and in person to ensure a broad reach. The questionnaire comprised several sections: Demographic Information: Questions on age, gender, education level, marital status, living alone, employment status, income level, financial situation, ethnicity, and addiction. The survey comprised 57 questions and was divided into six sections: Consent statement, general personal information, social engagement, scam vulnerability, cyber scam-related personal information, self-acceptance, and Well-being test. The survey used various Likert scales for different sections, measuring aspects like social engagement, scam vulnerability, self-acceptance, and well-being. Notable scales included those by Ueno et al. (2022) for scam vulnerability, Ryff for self-acceptance, and the W-BQ12 by Prof. Clare Bradley. However, the latter needed validation in Singapore (Mitchell & Bradley, 2001).

Cyber Scam Experience: Questions to determine if the participant had ever been a victim of a cyber scam. Social Engagement: Questions to assess the level of social engagement, including frequency of social interactions, participation in community activities, and presence in online social networks. Pearson Chi-Square Test (Hypothesis H0 1): Used to assess the correlation between demographic variables and susceptibility to cyber scams among Singapore-based participants. This test is suitable for categorical data and helps determine if there are significant associations between variables. Spearman's Correlation Test (Hypothesis H0 2): Employed to explore the relationship between social engagement (an or-

dinal variable) and being a cyber scam victim. This non-parametric test is used when data do not necessarily follow a normal distribution, measuring the strength and direction of association between two ranked variables. A total of 302 respondents participated in the survey. Two were excluded for failing to complete the consent form, leaving 300 completed responses for analysis. The survey was conducted online using Google Forms and was available in English and Mandarin. Participation was anonymous, and the survey was unavailable in Malay and Tamil. The study was conducted following ethical guidelines. Participants were informed about the purpose of the study, the voluntary nature of their participation, and the confidentiality of their responses. Informed consent was obtained from all participants.

7. Results

This descriptive study predominantly involved participants from Singapore, with 88% (n = 266) residing there. The gender distribution was closely aligned with the national average reported by the Singapore Department of Statistics, consisting of 50.8% male and 49.2% female participants. A significant portion of the participants, 70.7%, were between the ages of 30 and 50 years, reflecting the median age in Singapore. Hypothesis Testing Hypothesis H0 1: Examined the correlation between demographic factors (including gender, age, education, marital status, and others) and susceptibility to being a victim of scams. Hypothesis H0 2: Investigated the relationship between social engagement and cyber scam victimization.

Normality: To start with the analysis it was pertinent to check whether data was normally distributed or not, so that it could be decided that parametric methods are suitable or non-parametric. As it can be noted from **Table 1** that all continuous/scale variables had skewness within ±1 (Hair, Black, Babin, & Anderson, 2006) and kurtosis values within ±2 (Garson, 2012), thus the use of parametric methods was justified.

Reliability: Reliability analysis showed that Self-Acceptance (Section 5) had the Cronbach alpha > 0.7 (Hair et al., 2006) while others didn't meet this criterion (**Table 1**). M and SD scores are also given in **Table 1** for descriptive purposes.

Table 1. Data descriptive, reliability and normality.

					Skewness		Kurtosis	
	No. of Questions	Cronbach's α	M	SD	Statistic	SE	Statistic	SE
Overall (*n = 300*)								
Section 2	7	0.629	22.31	3.52	0.091	0.141	0.063	0.281
Section 3	9	0.380	21.50	2.93	0.454	0.141	1.242	0.281

Continued

Section 5	12	0.805	48.05	7.27	0.004	0.141	−0.521	0.281
Section 6	12	0.544	22.19	3.91	−0.110	0.141	−0.386	0.281
SG (*n* = *266*)								
Section 2	7	0.626	21.79	3.93	0.157	0.149	−0.361	0.298
Section 3	9	0.408	21.65	3.00	0.381	0.149	1.140	0.298
Section 5	12	0.806	47.76	7.35	0.073	0.149	−0.505	0.298
Section 6	12	0.569	22.12	3.91	−0.089	0.149	−0.295	0.298
nSG (*n* = *34*)								
Section 2	7	0.667	21.03	4.20	−0.493	0.403	0.708	0.788
Section 3	9	−0.438	20.26	1.88	0.173	0.403	0.083	0.788
Section 5	12	0.777	50.26	6.35	−0.526	0.403	0.043	0.788
Section 6	12	0.154	22.68	3.85	−0.279	0.403	−1.080	0.788

M = mean, SD = standard error, SE = standard error.

Table 2. Age and scam victim crosstabulation.

Q2			Q29		
			Not Victim	Yes Victim	Total
Yes	Q1	20 - 30 Years	24_a	5_a	29
		30 - 40 Years	72_a	12_a	84
		40 - 50 Years	95_a	9_a	104
		50 - 60 Years	37_a	4_a	41
		60 - 70 Years	7_a	0_a	7
		>70 Years	1_a	0_a	1
	Total		236	30	266
No	Q1	20 - 30 Years	6_a	0_a	6
		30 - 40 Years	7_a	0_a	7
		40 - 50 Years	12_a	1_a	13
		50 - 60 Years	4_a	0_a	4
		60 - 70 Years	1_a	1_b	2
		>70 Years	1_a	1_b	2
	Total		31	3	34

Each subscript letter denotes a subset of Q29 categories whose column proportions do not differ significantly from each other at the 0.05 level.

As shown in Table 2, it presents descriptive statistics for different sections of the survey among all participants, Singapore residents (SG), and non-Singapore residents (nSG). The statistics include the number of questions (No. of Questions),

Cronbach's alpha (Cronbach's α), mean (M), standard deviation (SD), skewness, and kurtosis. Standard errors (SE) are reported for skewness and kurtosis. For the overall sample (n = 300), Section 2 (Social Engagement) consisted of 7 questions, showing a Cronbach's alpha of 0.629, a mean score of 22.31, and a standard deviation of 3.52. Skewness was 0.091 (SE = 0.141), and kurtosis was 0.063 (SE = 0.281). Section 3 (Scam Vulnerability) comprised 9 questions, with a lower reliability (Cronbach's alpha = 0.380), a mean of 21.50, and a standard deviation of 2.93. This section showed more positive skewness (0.454) and higher kurtosis (1.242). Section 5 (Self-Acceptance) had 12 questions, demonstrating high reliability (Cronbach's alpha = 0.805), a mean of 48.05, and a standard deviation of 7.27. It exhibited negligible skewness and negative kurtosis. Section 6 (Wellbeing) also included 12 questions, with a Cronbach's alpha of 0.544, a mean of 22.19, and a standard deviation of 3.91. Among Singapore residents (SG, n = 266), similar patterns were observed with slight variations in means and standard deviations. For non-Singapore residents (nSG, n = 34), the reliability coefficients varied more substantially across sections, with notable differences in means and standard deviations.

A crosstabulation was conducted to examine the relationship between age groups and scam victim status among participants. The sample was divided based on their response to whether they had been a victim of a scam ("Yes Victim" vs. "Not Victim") and their age group. The age groups were categorized as 20 - 30 years, 30 - 40 years, 40 - 50 years, 50 - 60 years, 60 - 70 years, and over 70 years. The total number of participants was 300, with 266 responding "Yes" to having been a scam victim and 34 responding "No". Among those who reported being a victim of a scam (N = 266), the majority were in the 40 - 50 years age group (n = 104), followed by the 30 - 40 years (n = 84), 50 - 60 years (n = 41), 20 - 30 years (n = 29), 60 - 70 years (n = 7), and over 70 years (n = 1). The number of scam victims in each age group was 5, 12, 9, 4, 0, and 0, respectively. In contrast, among those who reported not being a victim of a scam (N = 34), the highest number was in the 40 - 50 years age group (n = 13), followed by 20 - 30 years and 50 - 60 years (each n = 6), 30 - 40 years (n = 7), 60 - 70 years (n = 2), and over 70 years (n = 2). The number of non-victims in each age group was 6, 7, 12, 4, 1, and 1, respectively. Post hoc comparisons using the Tukey HSD test indicated that there were no significant differences at the 0.05 level in the column proportions for each age category, denoted by subscript letters (a, b) as shown in Table 3.

Chi-Square tests were conducted to assess the relationship between age and scam victim status among 300 individuals divided into victims (n = 34) and non-victims (n = 266). For victims, the Pearson Chi-Square ($\chi^2 = 3.618$, df = 5, $p = 0.606$) and Likelihood Ratio ($\chi^2 = 4.397$, df = 5, $p = 0.494$) indicated no significant association between age and scam victimization. However, the Linear-by-Linear Association showed a marginal trend ($\chi^2 = 2.878$, df = 1, $p = 0.090$).

Table 3. Chi-square test—age and scam victim.

Q2		Value	df	Asymptotic Significance (2-sided)
Yes	Pearson Chi-Square	3.618[a]	5	0.606
	Likelihood Ratio	4.397	5	0.494
	Linear-by-Linear Association	2.878	1	0.090
	N of Valid Cases	266		
No	Pearson Chi-Square	10.096[b]	5	0.073
	Likelihood Ratio	7.698	5	0.174
	Linear-by-Linear Association	5.927	1	0.015
	N of Valid Cases	34		

[a]5 cells (41.7%) have expected count less than 5. The minimum expected count is 0.33. [b]5 cells (41.7%) have expected count less than 5. The minimum expected count is 0.11.

For non-victims, the Pearson Chi-Square approached significance ($\chi^2 = 10.096$, df = 5, $p = 0.073$), while the Likelihood Ratio did not suggest a significant relationship ($\chi^2 = 7.698$, df = 5, $p = 0.174$). Notably, the Linear-by-Linear Association was significant ($\chi^2 = 5.927$, df = 1, $p = 0.015$), indicating a trend across age groups.

Both tests noted potential issues with low expected counts in 41.7% of cells, which may affect the robustness of the results (as shown in **Table 4**).

Table 4. Ethnicity and scam victim crosstabulation.

Q2			Q29		Total
			Not Victim	Yes Victim	
Yes	Q4	Caucasian	4_a	1_a	5
		Chinese	181_a	23_a	204
		Filipino	11_a	0_a	11
		Indian	22_a	2_a	24
		Malay	7_a	2_a	9
		Prefer not to Say	10_a	2_a	12
		Others	1_a	0_a	1
		Total	236	30	266
No	Q4	Caucasian	15_a	1_a	16
		Chinese	8_a	1_a	9
		Filipino	1_a	0_a	1
		Indian	0_a	1_b	1
		Malay	1_a	0_a	1
		Prefer not to Say	4_a	0_a	4
		Others	2_a	0_a	2
		Total	31	3	34

Each subscript letter denotes a subset of Q29 categories whose column proportions do not differ significantly from each other at the 0.05 level.

8. Ethnicity and Scam Victim Status

A crosstabulation was conducted to explore the relationship between participants' ethnicity and their scam victim status. Participants were categorized by their self-identified ethnicity (Caucasian, Chinese, Filipino, Indian, Malay, Prefer not to Say, Others) and whether they had been a victim of a scam ("Yes Victim" vs. "Not Victim"). The total sample consisted of 300 participants. Among participants who reported being a scam victim (Yes Victim, N = 266), the following distribution was observed: 181 identified as Chinese, 22 as Indian, 11 as Filipino, 7 as Malay, 4 as Caucasian, 10 preferred not to say, and 1 identified as Other. The number of scam victims within each ethnic group was 23 for Chinese, 2 for Indian, 0 for Filipino, 2 for Malay, 1 for Caucasian, and 0 for the other category. Conversely, among those who reported not being a scam victim (No Victim, N = 34), the distribution was as follows: 15 Caucasians, 8 Chinese, 1 Filipino, 1 Indian, 1 Malay, 4 preferred not to say, and 2 identified as Other. The number of non-victims within each ethnic group was 1 for Chinese, 1 for Indian, 0 for Filipino, 0 for Malay, 1 for Caucasian, and 0 for the Other category. Post hoc comparisons using the Tukey HSD test indicated that there were no significant differences at the 0.05 level in the column proportions for each ethnicity category, denoted by subscript letters (a, b) as shown in Table 5.

Table 5. Education and scam victim crosstabulation.

Q2			Q29		Total
			Not Victim	Yes Victim	
Yes	Q5	Secondary School	21_a	6_a	27
		College/Polytechnic	60_a	4_a	64
		University	155_a	20_a	175
		Total	236	30	266
No	Q5	Secondary School	2_a	0_a	2
		College/Polytechnic	5_a	1_a	6
		University	24_a	2_a	26
		Total	31	3	34

Each subscript letter denotes a subset of Q29 categories whose column proportions do not differ significantly from each other at the 0.05 level.

A crosstabulation was conducted to explore the relationship between participants' ethnicity and their scam victim status. Participants were categorized by their self-identified ethnicity (Caucasian, Chinese, Filipino, Indian, Malay, Prefer not to Say, Others) and whether they had been a victim of a scam ("Yes Victim" vs. "Not Victim"). The total sample consisted of 300 participants. Among participants who reported being a scam victim (Yes Victim, N = 266), the following distribution was observed: 181 identified as Chinese, 22 as Indian, 11 as Filipino, 7 as Malay, 4 as Caucasian, 10 preferred not to say, and 1 identified as Other.

The number of scam victims within each ethnic group was 23 for Chinese, 2 for Indian, 0 for Filipino, 2 for Malay, 1 for Caucasian, and 0 for the Other category. Conversely, among those who reported not being a scam victim (No Victim, N = 34), the distribution was as follows: 15 Caucasians, 8 Chinese, 1 Filipino, 1 Indian, 1 Malay, 4 preferred not to say, and 2 identified as Other. The number of non-victims within each ethnic group was 1 for Chinese, 1 for Indian, 0 for Filipino, 0 for Malay, 1 for Caucasian, and 0 for the Other category. Post hoc comparisons using the Tukey HSD test indicated that there were no significant differences at the 0.05 level in the column proportions for each ethnicity category, denoted by subscript letters (a, b) as shown in Table 6.

Table 6. Multiple correlations.

Q2	Q	Q1	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q29
	Q1	1										
	Q3	0.121*	1									
	Q4	−0.105	−0.020	1								
	Q5	−0.082	−0.035	0.017	1							
	Q6	−0.205**	0.054	−0.035	−0.101	1						
Yes	Q7	0.213**	0.004	−0.068	0.042	−0.704**	1					
	Q8	0.137*	0.096	−0.050	−0.129*	0.102	−0.068	1				
	Q9	0.113	0.015	−0.057	0.214**	−0.160**	0.102	−0.184**	1			
	Q10	0.016	0.034	−0.095	0.213**	−0.103	0.100	−0.050	−0.050	1		
	Q11	−0.015	−0.306**	−0.015	−0.214**	0.075	0.000	−0.049	−0.042	−0.179**	1	
	Q29	−0.104	−0.172**	0.020	−0.048	0.011	−0.063	0.006	−0.023	0.032	−0.028	1
N = 266, **$p < 0.01$												
	Q1	1										
	Q3	0.022	1									
	Q4	−0.305	0.117	1								
	Q5	−0.096	0.206	0.276	1							
	Q6	−0.263	0.000	0.162	−0.427*	1						
No	Q7	0.091	0.114	−0.134	0.294	−0.485**	1					
	Q8	−0.229	0.000	−0.128	−0.015	−0.065	−0.128	1				
	Q9	0.465**	−0.134	−0.019	0.160	−0.391*	0.083	−0.028	1			
	Q10	−0.073	−0.271	−0.315	−0.180	0.034	0.063	−0.167	−0.386*	1		
	Q11	−0.057	−0.221	0.423*	0.068	−0.128	0.088	−0.159	−0.064	−0.037	1	
	Q29	0.424*	−0.104	−0.021	−0.021	−0.225	−0.043	−0.070	0.276	0.034	0.226	1
N = 34, *$p < 0.05$.												

For Singapore residents, a significant correlation between gender and scam victimization was found ($\chi^2(1) = 7.848$, $p = 0.005$), contradicting Hypothesis H0 1 for this demographic. The financial situation, although positively correlated, was not significant, supporting the H01. For non-Singapore residents, significant

correlations were observed in addiction and scam victimization, challenging H0 1 in this aspect. The detailed results of this analysis are presented in Table 6. Further analysis using Pearson correlation (Table 6) indicated gender as a significant factor in scam victimization for Singapore residents, while age was more influential for non-Singapore residents. A Pearson correlation analysis was conducted to assess the relationships between various factors and scam victimization among participants. The analysis focused on different demographic and personal characteristics for residents of Singapore and those not based in Singapore.

Findings for Singapore-Based Residents:

1) "For residents of Singapore, the analysis revealed a significant negative correlation between gender and being a victim of scams ($r = -0.172$, $p < 0.01$). This indicates that gender was a significant predictor of scam victimization in this group, with one gender being more susceptible than the other."

2) "Interestingly, the financial situation was found to have the highest positive correlation with being a scam victim ($r = 0.032$); however, this correlation was not statistically significant ($p > 0.05$), suggesting that financial status alone may not be a strong indicator of scam vulnerability in this population."

3) "No other factors examined showed a significant correlation with being a scam victim among Singapore-based residents."

Findings for Non-Singapore-Based Individuals:

1) "In contrast, for individuals not based in Singapore, age emerged as the most influential factor. The data suggested that older people were more susceptible to scams, indicating a significant relationship between age and scam victimization in this group."

2) "This finding underscores the importance of considering demographic variations, such as geographic location, when analyzing susceptibility to scams."

Hypothesis H0 2: There is no correlation between social life (social engagement) and being a cyber scam victim. The Spearman's correlation test showed and scam victim were negatively correlated ($r = -0.045$, $p = 0.466$) and that the correlation was non-significant, thereby supporting the H0 for the Singapore-based participants (as shown in Table 7).

Table 7. Social engagement and scam victim correlation.

Q2			Value	Asymptotic Standard Error[a]	Approximate T[b]	Approximate Significance
Yes	Interval by Interval	Pearson's R	−0.026	0.074	−0.422	0.673[c]
	Ordinal by Ordinal	Spearman Correlation	−0.045	0.068	−0.730	0.466[c]
	N of Valid Cases		266			
No	Interval by Interval	Pearson's R	−0.002	0.268	−0.012	0.990[c]
	Ordinal by Ordinal	Spearman Correlation	0.074	0.229	0.422	0.676[c]
	N of Valid Cases		34			

[a]Not assuming the null hypothesis. [b]Using the asymptotic standard error assuming the null hypothesis. [c]Based on normal approximation.

9. Correlation Analysis

"A Pearson's r correlation analysis was conducted to examine the relationship between social engagement and scam victimization. For respondents who answered 'Yes' in Q2, a very weak, negative correlation was found (r = −0.026, p = 0.673). A Spearman's ordinal correlation analysis yielded similar results (rs = −0.045, p = 0.466). Among respondents who answered 'No' in Q2, Pearson's r indicated no correlation (r = −0.002, p = 0.990), and Spearman's ordinal correlation showed a weak, positive correlation (rs = 0.268, p = 0.676). However, none of these correlations were statistically significant. The analyses were based on 266 cases for 'Yes' responses and 34 cases for 'No' responses." Based on this analysis, it can be concluded that there is no reliable evidence to suggest that social engagement is related to the likelihood of being a victim of a scam, as measured in this study.

10. Discussion

This study sought to unravel the complex interplay between various demographic and psychological factors and their correlation with susceptibility to cyber scams, specifically focusing on a Singapore-based cohort. The investigation, guided by two distinct hypotheses, revealed nuanced insights into the patterns and predictors of scam victimization. Analyzing demographic factors, including gender, age, education, marital status, and others about scam victimhood (Hypothesis H0 1) yielded intriguing findings. Contrary to our initial assumption of no significant correlations, a notable exception emerged: gender. Singapore-based male participants were more likely to fall victim to scams than their female counterparts. This finding contradicts some previous research suggesting that females might be more susceptible to certain types of scams, particularly those exploiting emotional or relational vulnerabilities, such as romance scams (Odunze, 2018). However, our results align with other studies indicating that males may be more prone to risks due to overconfidence in online environments or greater exposure to technology-driven fraud (Notté et al., 2021). The lack of significant correlations with other demographic factors suggests a complex interplay where no single factor dominantly predicts scam victimhood, underscoring the need for a multifaceted approach to cyber scam awareness and prevention strategies. Hypothesis H0 2, examining the relationship between social engagement and scam victimization, did not find a significant correlation. This outcome challenges the premise that higher social engagement inherently provides protective benefits against scams. Individuals with robust social networks might be better informed about scams and, thus, more vigilant. However, the results indicate that awareness and prevention of scams rely on more than just social engagement (Parti, 2022). This suggests that other factors, such as digital literacy, individual awareness, and the nature of social networks, might play more pivotal roles in influencing an individual's susceptibility to cyber

scams.

11. Implications for Cybersecurity Awareness and Policy

These findings have substantial implications for developing targeted cybersecurity awareness programs and policies. The gender-specific vulnerability suggests a need for tailored awareness campaigns that address the specific risks and behaviors predominant among males. The lack of correlation with social engagement and psychological factors points to the necessity of broad-based educational initiatives that transcend demographic and psychological boundaries. Awareness campaigns should be comprehensive, catering to diverse demographics and improving digital literacy and scam recognition skills (Wang et al., 2020).

12. Limitations and Future Research Directions

The study's focus on a specific geographic location (Singapore) provides an in-depth understanding of that context but may not fully represent global patterns. Cyber scams vary widely in approach and impact across different cultures and regions. Future studies should be conducted in diverse geographical and cultural settings. This would help determine whether the observed patterns are universal or specific to certain contexts. Investigating other factors like technological savviness or specific online behaviours could deepen the understanding of scam victimization. Different demographic groups may have varying levels of awareness or susceptibility to scams based on their digital literacy and online habits. An interesting area for further exploration is the examination of the values, beliefs, and motivations driving scammers. Understanding the psychology and circumstances of scammers could provide insights into more effective prevention strategies. Despite its limitations, the study importantly challenges some conventional assumptions about scam victimization and emphasizes its complex nature. It underscores the need for nuanced and practical approaches to scam prevention and digital safety education. In summary, while the study offers significant contributions to the understanding of factors influencing susceptibility to cyber scams, it also opens up avenues for more comprehensive research encompassing diverse contexts, additional influencing factors, and an exploration of the scammers' perspectives. This holistic approach can potentially lead to more effective prevention strategies and educational programs.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

Ajayi, T. M. (2022). Discursive-Manipulative Strategies in Scam Emails and SMS: The Nigerian Perspective. *Lodz Papers in Pragmatics, 18,* 175-195. https://doi.org/10.1515/lpp-2022-0008

Algharabat, R. S., & Rana, N. P. (2020). Social Commerce in Emerging Markets and Its Impact on Online Community Engagement. *Information Systems Frontiers, 23,* 1499-1520. https://doi.org/10.1007/s10796-020-10041-4

Bossler, A. M., & Berenblum, T. (2019). Introduction: New Directions in Cybercrime Research. *Journal of Crime and Justice, 42,* 495-499. https://doi.org/10.1080/0735648x.2019.1692426

Burton, A., Cooper, C., Dar, A., Mathews, L., & Tripathi, K. (2022). Exploring How, Why and in What Contexts Older Adults Are at Risk of Financial Cybercrime Victimisation: A Realist Review. *Experimental Gerontology, 159,* Article ID: 111678. https://doi.org/10.1016/j.exger.2021.111678

Carter, E. (2020). Distort, Extort, Deceive and Exploit: Exploring the Inner Workings of a Romance Fraud. *The British Journal of Criminology, 61,* 283-302. https://doi.org/10.1093/bjc/azaa072

Census of Population (2020). https://www.singstat.gov.sg/publications/reference#Census-of-Population-2020

Cheng, C., Chan, L., & Chau, C. (2020). Individual Differences in Susceptibility to Cybercrime Victimization and Its Psychological Aftermath. *Computers in Human Behavior, 108,* Article ID: 106311. https://doi.org/10.1016/j.chb.2020.106311

Cole, T. (2022). Exploring Fraudsters Strategies to Defraud Users on Online Employment Databases. *International Journal of Cyber Criminology, 16,* 61-86.

De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2021). What We Think We Know about Cybersecurity: An Investigation of the Relationship between Perceived Knowledge, Internet Trust, and Protection Motivation in a Cybercrime Context. *Behaviour & Information Technology, 41,* 1796-1808. https://doi.org/10.1080/0144929x.2021.1905066

Fong, C., & Tripathi, S. (2021). Multicultural Workplace Counselling and the Impact of Wealth, Health, Ability and Time (WHAT) on Mental Health under COVID-19 Pandemic. *Psychology, 12,* 1743-1755. https://doi.org/10.4236/psych.2021.1211105

Garson, G. D. (2012). *Testing Statistical Assumptions*. Statistical Associates Publishing.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., Palmatier, R. W., Dant, R. P., Grewal, D., & Evans, K. R. (2006). Factors. *Marketing, 41,* 1146-1172.

H. M. Buse, J., Ee, J., & Tripathi, S. (2023). Unveiling the Unseen Wounds—A Qualitative Exploration of the Psychological Impact and Effects of Cyber Scams in Singapore. *Psychology, 14,* 1728-1742. https://doi.org/10.4236/psych.2023.1411101

Johnson, M. P., & Leone, J. M. (2005). The Differential Effects of Intimate Terrorism and Situational Couple Violence: Findings from the National Violence against Women Survey. *Journal of Family Issues, 26,* 322-349.

Lubben, J., Gironda, M., Sabbath, E., Kong, J., & Johnson, C. (2015). *Social isolation presents a grand challenge for social work. Grand Challenges for Social Work Initiative.* Working Paper No. 7.

Maimon, D., Santos, M., & Park, Y. (2019). Online Deception and Situations Conducive to the Progression of Non-Payment Fraud. *Journal of Crime and Justice, 42,* 516-535. https://doi.org/10.1080/0735648x.2019.1691857

Mekler, J. (2022). *Mental Well-Being of Generation Z as Potential Victims of Cybercrime: The Effect of Risk Perception and Self-Efficacy on Mental Well-Being.* Ph.D. Thesis, University of Twente.

Mitchell, J., & Bradley, C. (2001). Psychometric Evaluation of the 12-Item Well-Being Questionnaire for Use with People with Macular Disease. *Quality of Life Research, 10,*

465-473. https://doi.org/10.1023/a:1012540100613

Notté, R., Leukfeldt, E. R., & Malsch, M. (2021). Double, Triple or Quadruple Hits? Exploring the Impact of Cybercrime on Victims in the Netherlands. *International Review of Victimology, 27,* 272-294. https://doi.org/10.1177/02697580211010692

Odunze, D. (2018). Cyber Victimization by Hackers: A Criminological Analysis. *Public Policy and Administration Research, 8,* 8-15.

Parti, K. (2022). "Elder Scam" Risk Profiles: Individual and Situational Factors of Younger and Older Age Groups' Fraud Victimization. *International Journal of Cybersecurity Intelligence & Cybercrime, 5,* 20-40. https://doi.org/10.52306/2578-3289.1117

Ueno, D., Arakawa, M., Fujii, Y., Amano, S., Kato, Y., Matsuoka, T. et al. (2022). Psychosocial Characteristics of Victims of Special Fraud among Japanese Older Adults: A Cross-Sectional Study Using Scam Vulnerability Scale. *Frontiers in Psychology, 13,* Article 960442. https://doi.org/10.3389/fpsyg.2022.960442

Wang, P., Su, M., & Wang, J. (2020). Organized Crime in Cyberspace: How Traditional Organized Criminal Groups Exploit the Online Peer-to-Peer Lending Market in China. *The British Journal of Criminology, 61,* 303-324. https://doi.org/10.1093/bjc/azaa064