Scientific Research Publishing

Psychology, 2023, 14, 1728-1742
https://www.scirp.org/journal/psych
ISSN Online: 2152-7199
ISSN Print: 2152-7180

Unveiling the Unseen Wounds—A Qualitative Exploration of the Psychological Impact and Effects of Cyber Scams in Singapore

Johan H. M. Buse[1], Jonathan Ee[2], Shilpi Tripathi[3]*

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

How to cite this paper: Buse, J. H. M., 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

Received: September 25, 2023
Accepted: November 27, 2023
Published: November 30, 2023

Abstract

Introduction: In a world where the virtual realm is integral to daily life, facilitating communication, commerce, and social interactions, the rise of the digital landscape has brought both unprecedented opportunities and new challenges. Among these challenges, cyber scams have emerged as a modern affliction that transcends geographical boundaries, targeting individuals with precision and cunning. **Objective:** A Qualitative Exploration: The essence of this study lies in its commitment to unveiling the unseen wounds inflicted by cyber scams. Unlike quantitative studies prioritizing statistical generalizability, our qualitative research embraces the richness of individual narratives, emphasizing diverse responses and the uniqueness of each victim's journey. **Methodology:** Mapping Emotional Labyrinths: Drawing on in-depth interviews, personal accounts, and narrative analysis, we aim to map the intricate labyrinth of emotions that unfold when trust is betrayed, security is shattered, and one's digital reality transforms into a nightmare. **Conclusion:** This study seeks to transcend the limitations of numbers, offering insights into the profound realms of human emotion, perception, and meaning-making in the aftermath of cyber scams. Resilience, Healing, Empowerment: By walking hand in hand with our participants, we aim to illuminate the path toward resilience, healing, and empowerment. The ultimate goal is to foster a more secure and psychologically robust digital society.

Keywords

Cyber Scams, Digital Cheating, Scam Victims, Psychological Exploitation, Multicultural

*Corresponding author.

1. Introduction

In an era of digital interconnectedness, the virtual realm has become integral to daily life, facilitating communication, commerce, and social interactions. The rise of this digital landscape has expanded the horizons of human potential and introduced novel avenues for exploitation (Agrafiotis et al., 2018). Among these challenges, cyber scams have emerged as a modern-day affliction that transcends geographical boundaries, targeting individuals with unprecedented precision and cunning (Button et al., 2009).

While considerable attention has been paid to cyber scams' technical and financial aspects, a pivotal yet often overlooked dimension is the profound psychological toll they exact on their victims (Alsawalqa, 2021). This qualitative study delves into the intricate tapestry of emotions, cognition, and behavior that shape the lived experiences of individuals who have fallen prey to cyber scams. By embracing a qualitative approach, we seek to unmask the intricate layers of the psychological aftermath, allowing a nuanced understanding of the complex interplay between technology-mediated deceit and the human psyche (Hsu & Willis, 2013).

The essence of this study lies in its commitment to unveil the unseen wounds inflicted by cyber scams. Unlike quantitative studies that often prioritize statistical generalizability, qualitative research embraces the richness of individual narratives, highlighting the diversity of responses and the uniqueness of each victim's journey (Cheng et al., 2020). In doing so, we aim to transcend the limitations of numbers and delve into the depths of human emotion, perception, and meaning-making, shedding light on the complex ways cyber scams reverberate within the human soul (Cohen et al., 1981). Through this qualitative exploration, we intend to enrich the academic discourse on cybercrime and offer a platform for the voices of those who have endured its psychological reverberations. By engaging with victims' personal stories, coping mechanisms, and recovery trajectories, we can gain profound insights into the human dimensions of cyber scams—insights that can inform holistic strategies in the following sections, we embark on a journey through the experiences of individuals who have encountered the treacherous landscapes of cyber scams. Drawing on in-depth interviews, personal accounts, and narrative analysis, we map the intricate labyrinth of emotions that unfold when trust is betrayed, security is shattered, and one's digital reality transforms into a nightmare (Burton et al., 2022). By walking hand in hand with our participants, we aim to illuminate the path toward resilience, healing, and empowerment, fostering a more secure and psychologically robust digital society (Howell et al., 2019).

2. Methodology

Based on Braun and Clarke's thematic analysis approach, reflexive thematic analysis guided data analysis (Clarke et al., 2015). The transcripts were uploaded and analyzed using the cloud-based qualitative analysis software. Two research-

ers (JB & JE) met weekly in the early phases of data collection to reflect on the process of data collection and early patterns of analysis. Throughout the analytical process, participants applied reflexivity by discussing their relationship to and interest in the research topic and reflecting on how their academic, professional, and personal backgrounds affected the interpretation of data. Following data collection and preliminary analysis, team members read full transcripts and discussed key concepts for the codebook development process. Team researchers (JB & JE) analyzed the first set of transcripts iteratively to generate codes. All team members became familiar with the data as data collection and preliminary analysis progressed by reading full transcripts and outlining key concepts for the codebook development process. A team of researchers reviewed and developed the themes (JB & JE). In the process of writing up results and weaving participant data (quotations) into an analytical narrative, themes were finalized. The thematic analysis involves systematically identifying, organizing, and looking into patterns of meaning (themes) across the dataset, allowing the researcher to visualize and make sense of shared or collective meaning and experiences (Clarke et al., 2015).

Moreover, the thematic analysis comprised six steps; becoming familiar with the data, generating initial codes, generating themes, reviewing themes, defining themes, and finally, the write-up. The data were transcribed verbatim on a Word document by listening to the interviews. The data was coded by examining the transcribed data. This allowed us to identify common themes such as ideas, topics, and repeated patterns, such as lack of resources and support. The themes were then reviewed to ensure they accurately represented the data. Lastly, the various themes were renamed for easier.

2.1. Ethical Considerations and Safeguards for Participants

Informed Consent:

Before participating in the study, all participants were fully informed about the nature, purpose, and potential impact of the research. Informed consent forms were provided and thoroughly explained, ensuring that participants understood their rights and could make an informed decision about their involvement.

2.2. Anonymity and Confidentiality

To protect the privacy of participants, all collected data was anonymized. Personal identifiers were removed or pseudonyms were used in reporting findings. The data was securely stored and accessible only to the research team. Participants were offered the opportunity to debrief after their involvement in the study. This session provided clarification on the research aims and offered support if the research process had elicited any emotional responses. Participation in the study was entirely voluntary, and participants could withdraw at any stage without consequences. They were made aware of their right to withdraw and

how to do so.

3. Recruitment of Candidates

A total of 16 candidates have participated in one-on-one interviews. Participants in the qualitative research ranged in age from 14 to 65. Seven males and nine females were interviewed. The research was not conducted on one candidate because they did not consent. All were residents of Singapore at the time of the (attempted) scam. Online and social media channels and platforms, including Facebook, Workplace, and WhatsApp, as well as online marketplaces, such as Carousel, were used to recruit candidates. As part of the survey, a residency-related question was included to ensure that data related to Singapore residents could be analyzed.

4. Research & Findings

4.1. Main Theme 1: Scamming Method

Scamming involves deceptive practices aimed at tricking individuals or organizations for financial gain. It includes fraudulent schemes, confidence tricks, and manipulative tactics that exploit trust or vulnerabilities. Scams can occur through various channels, such as online platforms, phone calls, or emails. Scammers use deceitful means to induce victims to part with money, sensitive information, or valuables.

In our qualitative study, we identified several ways in which individual personality traits and dispositions influenced participants' susceptibility to scams. Those with inherently lower levels of trust tended to be more skeptical, making them less likely to fall for scams, while individuals with a trusting disposition were found to be more vulnerable to deceptive tactics. Personality traits associated with a high tolerance for risk, such as adventurousness or impulsivity, correlated with a greater likelihood of engaging in risky financial endeavors, making participants more susceptible to scams promising high returns. Additionally, participants driven by a strong desire for financial gain or a sense of urgency were more prone to scams that appealed to their aspirations, sometimes leading them to overlook warning signs and engage in risky transactions. Emotional vulnerability, including a need for social connection, made individuals more susceptible to scams exploiting their emotions, often preying on feelings of loneliness, fear, or desperation. Those with a more impressionable disposition, influenced by external pressures or persuasive techniques, were also found to be more susceptible to scams employing manipulative tactics. Conversely, personality traits associated with a higher level of financial literacy, such as analytical thinking and skepticism, acted as protective factors, reducing the likelihood of falling victim to scams.

By examining these aspects, we aim to provide a nuanced understanding of how individual differences in personality and disposition can shape the dynamics of the scamming process. It is essential to recognize that these findings are

context-specific and may not universally apply, emphasizing the importance of tailoring anti-scam interventions to individual characteristics. One of the first critical themes from the interviews concerned the refinement and variety of scammers' emotional tools and techniques. Although many of the scams were found to have been conducted using similar modus operandi, each scam was conducted uniquely and driven by the victim's behavior. Personality and disposition played essential roles in the scamming process. It also became apparent that relationships played an important role in the scamming process. It was found that victims' friends unknowingly introduced the victims to scams and that scammers exploited relationships to scam the victims. It was also observed that, of the 16 interviewed participants, four were successful in avoiding financial loss. These participants detected their respective scams during the scamming process. It is impossible to provide a conclusive reason why these participants identified their respective scams promptly. Additionally, it was observed that three out of the four participants exhibited hypervigilance and demonstrated a lack of trust.

Subtheme* 1: *Psychological Elements Exploited by Scammers

The scammers exploited the victims' impulses, urgencies, and desires to trick them. The scammers also sought to build trust. As part of the job or investment scams, it is not uncommon for scammers to make payouts initially; after that, their victims become convinced of the legitimacy of the setup and are eventually tricked into paying large amounts of money. Many of the victims in this study were scammed owing to their desire for more, driven by ambition and a wish to improve their financial situations or secure advantageous deals.

These findings are discussed in more detail subsequently. It was also found that the scammers created "classes," such as silver, gold, and platinum, to appeal to the aspirations and ambitions of the individuals to be rewarded. Further, the victims of several investment and job scams stated that they were "performing tasks given by the leader or task manager":

- *So I was just watching a YouTube video, and they're reviewing an iPhone* 12, *and, in the comments, he was, like,* "*WhatsApp me on this number,*" *and I'm, like,* "*Okay,*" *and then I, like, basically WhatsApp, and then it's, like,* "*I can ship the iPhone close to you, just feeling like* $100, *and I'll ship it all,*" *and he's, like,* "*You have to pay a bit more,*" *and then he kept on asking repeatedly for me to give him more money, so my dad just, like, said,* "*We are not interested.*" (*Interviewee* 1)
- *Actually, half the price of what I saw in stores, so it sounded like a good deal I… When it was delivered to me, it was just an empty envelope. So, basically, the first one was where I saw an advertisement on Facebook regarding business costs that were able to give me financial freedom, so I signed up for it.* (Interviewee 3)

Subtheme* 2: *Personality and Disposition

This study asked the participants about their upbringing, family situations, and happiness. It was also observed that, in many cases, the victims knew other

victims (because some were involved in the same scam, typically investment scams). Some participants were victims of or exposed to more than one scam. The victims could be categorized as driven by ambition (i.e., with a necessity or desire to earn more), cooperative, and accommodating. In some cases, the victims' insecurity was evident during the interviews. Several participants expressed unhappiness with their current lives and due to their childhoods.

Conversely, in some cases, the victims expressed that they were happy and supportive, which resulted in their becoming victims of impersonation scams. In other situations, the fear of authority and desire to comply with the rules and regulations of banks led to several of the participants almost being scammed. The personality above traits are often exploited in various scams, such as impersonations of officials calling victims to instill fear about apparent security breaches, nonpaid fines, and lost credit card claims. Impulse and habit were traits expressed in some of the scam cases. So-called lock-in techniques are frequently used in investment and job scams. Victims invest or pay money and, to avoid losing their investments, are encouraged to continue investing to obtain more significant returns or payouts. Some of the participants considered themselves to be vigilant and rebellious. These participants were typically more alert and used self-taught verification techniques to assess legitimacy before acting on an offer. Several scam victims were scammed more than once, indicating some form of vulnerability. These were typically scams or unsuccessful scam attempts across various types of scams. Interviewee 3 revealed that they were scammed multiple times, with most of the scams seemingly resulting from the interviewee's greed. Interviewee 8 revealed they were exposed to multiple scam attempts but did not incur any financial losses. It was observed that this participant was hesitant and somewhat naïve. Interviewee 14, who revealed that they did lose money, came across as somewhat confused and insecure.

An SMS they sent to me because of the fact that I've been looking at the One Motoring website to see the cost rate…that I clicked on the website and it actually brought me…I'm very anxious. What can I do? (*Interviewee* 14)

Subtheme* 3: *Relationships and Culture

Singaporean society has a peculiar term: "kiasu," which is the fear of losing out. Relationships play a role in referring friends and family to seemingly good opportunities to make money. Relationships also play a significant role in impersonation scams, where victims fear their accounts have been hacked. Several of the participants described themselves as lonely, introverted, and seeking distraction in additional jobs:

I was trying to get the air conditioners cleaned, and do our regular maintenance, and that was during Chinese New Year, so we were trying to get it done before Chinese New Year, and the company was trying to fit in a schedule for that to come by, and I was getting a bit edgy because they couldn't fit me in. (*Interviewee* 11)

Subtheme* 4: *Scam Avoidance Versus Multiple Scams

Four participants (Participants 2, 8, 9, and 11) displayed alertness, which, ul-

timately, would have allowed them to avoid being scammed. These participants detected their respective scams during the scamming process. However, it was observed that three of the four participants were hypervigilant and had low trust levels, which indicated a form of perceived smartness and that they taught themselves mechanisms to verify legitimacy. In the interviews, these participants demonstrated high assertiveness and revealed that they took measures following their respective scam attempts. Some participants revealed that they were scammed or exposed to scam attempts multiple times (Participants 3, 8, 9, and 14). It was not possible to detect a pattern or common theme between these participants:

- *I always make it a point to Google pictures using some of the apps or software that I can find online to see if these people are real.* (*Interviewee*9)
- *So I let the person play the primary role in a conversation until I'm very sure that I can identify who they are before I actually let my guard down.* (*Interviewee* 11)

4.2. Main Theme 2: The Role of Online Platforms

In the last decade, fuelled by faster internet speeds, smartphones, and the rise of the "app-platform era", it has become easier to socially engage and trade, both for scammers and potential victims. The internet has become faster, and a new world of artificial enhancement and virtual reality is coming into play. Smartphones offer better features, such as inter alia, video calling, and, fuelled by all this, new platforms are emerging. Social media platforms, job platforms, and e-commerce platforms are all providing scammers with new ways to attempt to scam potential victims. A simple Google search and the scanning of public profiles on Facebook and other platforms can provide scammers with useful information. Generally, scammers use social media applications to contact potential scam targets and use the provided information to defraud their chosen victims.

Subtheme* 1: *Platform Society Creates a Real-Time, Fluid, Open, and Possibly Exposed Environment.

The term "platform society" refers to the new way of working and socializing using applications that offer direct access to a broad global audience. In addition to social media applications, such as Facebook, Instagram, and Snapchat, there are dedicated communication platforms, such as WhatsApp and Telegram; dating applications, such as Tinder, Coffee Meets, and Bagel; and collaboration platforms, such as Quest. The commonalities between all applications are the low entry barrier for anyone to join or use them, the limited possibility to verify user identities, and the ability to create subgroups or communities within the applications. Scammers use various applications and platforms to seek potential victims, communicate with the victims during the scamming process, and conduct their scams through group chats where they encourage their victims to, among other things, set up wallets and make payments. The digital prerogative is easy and immediate and constitutes low-barrier access to information, enabling fraudsters to find potential victims. In addition to easy access to information,

digital platforms offer real-time, direct, and personal communication opportunities. Such platforms further allow users to communicate via video and group chats. These communication channels can be used to pressure victims during the scamming process or into being part of the scam (extortion).

So I was just watching a YouTube video, and they're reviewing an iPhone 12, *and, in the comments, it was, like,* "*WhatsApp me on this number.*" (*Interviewee* 1) *So basically, the first one was when I saw an advertisement on Facebook regarding business costs that were able to give me financial freedom.* (*Interviewee* 3)

Subtheme* 2: *The Art of Faking: What Is Real in the Digital World?

Not only do digital platforms provide scammers with easy access to information about potential targets and direct access to potential victims, but they also allow scam perpetrators to mislead their victims by creating a fake virtual world. Fake identities on social media platforms, fake reviews, and "dress-up" websites are all tools that scammers use to mislead victims and convince victims of the legitimacy of their scams. In some cases, even during the scamming process, collaborators of the scam syndicate are used to apply peer pressure on victims to continue to participate and provide funds. These can be used to pressure victims during the scamming process or into being part of the scam (extortion). Following the completion of a scam, fraudsters often disappear into thin digital air; funds are often transferred overseas; in many cases, digital evidence is inaccessible to victims, as they are blocked from groups.

So that time I was like privately Telegram the other two candidates who were also in the chat with me because they were also making the payments, so I did personally ask them. I said, "*Hey, do you like receiving your funds after you pay your taxes and all these things?*" *But one of them told me yes, and, after, they immediately left the group chat. The other didn't reply, so I'm not sure whether they are actually, like, part of the gang or something like that.* (*Interviewee* 5)

4.3. Main Theme 3: Financial and Emotional Impacts of Scams

There was a wide variety among the participants regarding the discovery of the scams and the handling of the scams' emotional impact. Some participants said they were proud to have outsmarted their scammers by detecting the latter's malicious intentions in a timely manner. Others revealed that they experienced lengthy scamming processes but hoped that they would recover their losses. Many scammed participants said they felt ashamed, guilty, or stupid upon discovering the scams. Several of the participants filed police reports to attempt to recover their losses. Many attempts to recover losses via the police resulted in further disappointment, as recovery was impossible in almost all cases.

Subtheme* 1: *Discovery Process and Feelings

All the cyber scam victims expressed that they felt everything from dumb, disappointed, angry, embarrassed, and ashamed to shocked, scared, sad, upset, and lousy. In some cases, the financial losses were substantial, and trust was im-

pacted to such an extent that the victims were profoundly affected even long after the scams. Those who detected their scam attempts in time felt relieved and even proud. Some of the participants referenced others who were scammed to a worse extent than themselves:

- *I kind of felt dumb, I guess, for not realising it was a scam from the beginning.* (*Interviewee* 1)
- *I felt stupid. Why? Why? Why at that moment I didn't double check with my friends. Again.* (*Interviewee* 12)

Subtheme* 2: *The Process of Sharing and the Longer-Term Impact of Scams on Individuals' Mental Wellbeing

Indeed, it's accurate to acknowledge that some potential victims are more vigilant when it comes to the threat of scams. People who exhibit higher levels of vigilance are likely to be more cautious and skeptical, making it harder for scammers to succeed. This vigilance may stem from personal experiences, awareness of common scam tactics, or a general cautious mindset. Recognizing and understanding individual differences in vigilance is essential in developing effective strategies to prevent scams and enhance overall cybersecurity awareness. Others believe that, until late in the scamming process, they are doing something good with a reward at the end (e.g., financial benefits, good deals, etc.). Owing to the feelings that emerge when victims realize that they have been scammed, such as embarrassment, anger, and shame, victims often fear sharing their experiences with others. Victims fear being judged or, even worse, being scolded, as the following quote reveals:

…it's more on my wife. She has been feeling very, very bad over this, and, from time to time, she keeps crying whenever she thinks of this or when her friends actually mention the scam. You know, her parents actually tried to call her stupid for falling for this kind of scam. You're big, so how come you can still fall for this kind of scam? Yeah, so, like, everyone is blaming her, and then she also blames herself. How come she's not being more careful with things?… Then the parents also blame me by asking why I didn't stop my wife and things like that. (*Interviewee* 16)

Subtheme* 3: *Finding Ways to Avoid Being Scammed

After coming to terms with the scams, most participants revealed that they reflected on the events. The scam victims became more vigilant and took concrete action. This higher awareness increased the victims' intentions to verify presented information and take the initiative rather than waiting. Most participants eventually shared their experiences with friends, albeit reluctantly and belatedly. For most interviewees, being a scam victim or even being at risk of becoming a scam victim resulted in prolonged or permanent changes in trust and anxiety levels. The participants had various types of advice for others and themselves to avoid being scammed:

Now I don't make the first move and say, "Hey, is that you Ken?" I risk giving it away, so I let the person play the primary role in a conversation until I'm very sure that I can identify who they are before I actually let my guard down. (*Inter-*

viewee 11) *Do I really need to let go of my past? I mean my ID, my personal details? Yeah, so I will keep asking them, do you really need it? Yes. Only to the government department then I understand, okay, this is me they need they will have to fill. Yeah… Otherwise, I will be really conscious about letting go of my personal details.* (*Interviewee* 8)

5. Discussion

There is a limited amount of research on cyber scams. Most research on cyber scams relates to cybercrime, with most studies focusing on love scams (Carter, 2021; Wang & Topali, 2022) and fraudsters' methods (Carter, 2021). The present study aims to provide insights into the types of victims, scam processes, and their effects through quantitative research and qualitative insights. In the current study, victims' accounts of scams were systematically analyzed, and illustrative quotes were documented for each theme with detailed descriptions and discursive interpretations (Spradley, 1980). Similarly to Wang and Topalli's (Wang & Topalli, 2022) study, this study observed that scammers carefully engineered and staged their scamming processes. In the qualitative research of this study, the use of visceral triggers, the leveraging of social norms, the fabrication of crises by fraudsters, appeals to authority, impersonation, and the intelligent use of technology and platforms were observed. Not all the participants were scammed, with some detecting the threat during the scamming process. Others, however, did not detect the scam threat and experienced a protracted scamming process. Four of the participants avoided being scammed.

The qualitative study identified the psychological tactics that the scammers used. The tactics varied depending on the type of scam, with linguistic politeness and urgency cues being deployed in almost all cases. In the qualitative research of this study, the observed tactics confirmed the tactics that Williams et al. (Williams et al., 2017) described in their study. Fraudsters use linguistic politeness and language to sweet-talk their scam victims. Schaffer's (Schaffer, 2012) and Maimon et al.'s (2019) studies assessed the situational context of fraudsters' politeness. In these studies, scammers were found to have used various psychological tactics in their scams, such as emotionally appealing to victims for support, impersonating other people, provoking and exploiting scam victims' greed, triggering urgency, and applying peer pressure. Stajano and Wilson's (Stajano & Wilson, 2011) study described the principles to which victims respond: distraction, social compliance, herd (social proof), kindness, need and greed, and dishonesty. In the qualitative research of the present study, a range of scam sophistication levels were observed. According to Chang and Chang's (Chang & Chang, 2014) study, scammers' tactics and sophistication levels have evolved. Often, individuals unknowingly introduce their friends (potential future scam victims) to an unknown scam. This happens more frequently with investment scams. Scammers build victims' trust by using online tools, such as references, fake online reviews, and legitimate websites, to make their businesses seem

trustworthy. Regarding investment and job scams, fraudsters can make payouts to establish credibility. Regarding impersonation scams, fraudsters smartly use information about victims obtained from online platforms and utilize listening and question techniques during calls to obtain information that is then used to trick victims.

Regarding personality and disposition, in the qualitative research, several participants showed themselves to be obedient by nature, believed what was being shared, and complied with the instructions (Fong, 2021). A few participants highlighted that they were unhappy or had unhappy childhoods. Singapore is a competitive society for these participants, which could have been a factor in the scamming processes. Through their conformist behavior, when they were scammed, the participants were striving for financial betterment, which was motivated by greed (Cole, 2022a). In some instances, cultural elements and relationships either played a role in the scamming processes or influenced the participants' susceptibility to scams. In Bedford and Chua's (Bedford & Chua, 2018) study, "kiasuism" is described as a prominent Consumer scam. Victims were more likely to be women and those less educated. The quantitative results of the present study confirmed the gender correlation and that men were more prone to investment scams.

Online platforms support scammers' modus operandi in various ways. The qualitative research observed that scammers use various platforms in the scamming process, especially in investment, love, and job scams. Scammers maximize the various platforms' functionalities. WhatsApp, Facebook, and Tinder are used to source victims. Telegram and WhatsApp are used to communicate with victims (Bossler & Berenblum, 2019).

In some cases, groups are established to apply peer pressure. Scammers also seek to establish credibility online. Scammers write fake reviews and create profiles and websites to make potential victims believe a false truth. As fast as technology and platforms are developing and allowing scammers more advanced tools to conduct their scams, the Singapore government and online platforms worldwide are rapidly developing new tools to help identify and prevent scams. Lee's (Lee, 2022) study analyzed the tools leading e-commerce platforms use to detect and prevent scams.

The financial and emotional impacts of scams are substantial. Several participants highlighted that they were reluctant to and fearful of sharing their experiences with family and friends. Eventually, most participants shared their experiences, albeit more easily with friends than family, especially within households where sharing scamming experiences was considered difficult or taboo, owing to a fear of being blamed. Many participants blamed themselves and stated that they felt dumb, angry, embarrassed, and ashamed. For the participants, the emotional impact of the scams proved to be long-lasting. The quantitative research results confirmed the qualitative research observations, with a correlation between financial loss and type of scam (Cole, 2022b).

Further, quantitative and qualitative research results, which measured experienced feelings and emotions, were consistent. The investment scam victims tended to feel stupid; the impersonation and identity theft victims typically felt embarrassed; and the bank scam victims typically felt angry. In addition to victims blaming themselves, familial relationships were often adversely impacted by the scams over a long period, reducing well-being and victims' self-acceptance. Lerner's belief in a just world (BJW) theory is a helpful framework for understanding the blame that victims of online fraud face because it posits that behavioral responsibility (a trait commonly ascribed to online fraud victims) is central to perceived blameworthiness and that compensation for a crime determines the level of blame directed at victims (Kaakinen et al., 2018).

As victims of online fraud are exceptionally unlikely to receive any compensation, whether monetary or otherwise, the BJW theory can help to explain the blame directed at victims (De Keersmaecker & Roets, 2020). The interviewed scam victims indicated that they took time to accept their financial losses. Some of the victims were self-reflective and learned lessons from their ordeals, which they revealed that they have applied since their respective scam incidents, exhibiting behavioral changes. Moreover, the scammers' cross-border operating model would have made it impossible to recover financial losses. As unexpectedly as scammers can appear in victims' lives, they can disappear immediately (Button & Cross, 2017).

6. Conclusion and Recommendations

Qualitative research revealed the intricate techniques that fraudsters employ during the scamming process. Moreover, the research highlighted the complex and prolonged psychological effects of cyber scams on potential victims. The findings of this study could be used to prevent Singapore residents from becoming victims of cyber scams by using insights about segments (gender and age) related to scam types. By addressing specific signs and characteristics of the prevailing cyber scam types as identified in this research, government institutions can further improve cyber scam awareness and potentially increase prevention. By sharing (anonymised) testimonials of victims highlighting their insights and recommendations, cyber scam prevention can be further enhanced (Open AI, 2023).

Due to the taboo surrounding scams and the reluctance of victims to share their scam experiences, this research suggests two recommendations. As a result of feeling stupid and embarrassed, victims are afraid to share. Thus, these experiences and information cannot be used to raise awareness. Therefore, encouraging victims to share with institutions and through their social circles could help raise awareness and prevent cyber scams. To reduce the stigma caused by cyber scams, the second recommendation is to encourage institutions, profit and non-profit organizations to change the taboo of sharing cyber scam experiences. As a result, not only will more crimes be reported and shared, but victims' men-

tal well-being may also be improved (Akdemir & Lawlwss, 2020).

Singapore, renowned for its robust digital infrastructure and cyber-savvy residents, is well-positioned to further fortify its defenses against international scam syndicates. Building on their strengths, the Singapore government and its citizens can collaborate to elevate their vigilance and preparedness against cyber threats. This can include the deployment of advanced technological solutions to curb the access of foreign-based scam operators. Additionally, leveraging Singapore's strong educational framework, there could be a focus on enhancing critical thinking skills among residents. This initiative would be particularly effective in heightening awareness about impersonation scams, which often exploit a fear of authority. By continuing to nurture a culture of cyber awareness and resilience, Singapore can set a global example in effectively managing and mitigating the risks of cyber scams.

The reasons for the correlation between gender and cyber scams for Singapore residents should be further investigated and Further research should examine why some scam victims are scammed multiple times (Open AI, 2023). In light of the qualitative research findings and obtained insights, further in-depth studies on victims' mental well-being and the processing of cyber scams are recommended aiming to establish better victim aftercare. Cyber scam victims should not feel ashamed or victimized, and they deserve support to ensure that cyber scams no longer remain taboo.

Conflicts of Interest

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

References

Agrafiotis, I., Nurse, J. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate. *Journal of Cybersecurity, 4,* tyy006. https://doi.org/10.1093/cybsec/tyy006

Akdemir, N., & Lawless, C. (2020). Exploring the Human Factor in Cyber-Enabled and Cyberdependent Crime Victimisation: A Lifestyle Routine Activities Approach. *Internet Research, 30,* 1665-1687. https://doi.org/10.1108/INTR-10-2019-0400

Alsawalqa, R. (2021). Cyberbullying, Social Stigma, and Self-Esteem: The Impact of COVID-19 on Students from East and Southeast Asia at the University of Jordan. *Heliyon, 7,* e06711. https://doi.org/10.1016/j.heliyon.2021.e06711

Bedford, O., & Chua, S. (2018). Everything Also I Want: An Exploratory Study of Singaporean Kiasuism (Fear of Losing out). *Culture & Psychology, 24,* 491-511. https://doi.org/10.1177/1354067X17693831

Bossler, A., & 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

Braun, V., & Clarke, V. (2014). What Can "Thematic Analysis" Offer Health and Wellbeing Researchers? *International Journal of Qualitative Studies on Health and Well-Being, 9,* Article No. 26152. https://doi.org/10.3402/qhw.v9.26152

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 Victimization: A Realist Review. *Experimental Gerontology, 159,* Article ID: 111678. https://doi.org/10.1016/j.exger.2021.111678

Button, M., & Cross, C. (2017). *Cyber Frauds, Scams and Their Victims*. Taylor & Francis. https://doi.org/10.4324/9781315679877

Button, M., Lewis, C., Tapley, J. (2009). *Fraud Typologies and the Victims of Fraud Literature Review.* National Fraud Authority.

Carter, E. (2021). 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

Chang, J., & Chang, W. (2014). Analysis of Fraudulent Behavior Strategies in Online Auctions for Detecting Latent Fraudsters. *Electronic Commerce Research and Applications, 13,* 79-97. https://doi.org/10.1016/j.elerap.2013.10.004

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

Clarke, V., Braun, V., & Hayfield, N. (2015). Thematic Analysis. *Qualitative Psychology: A Practical Guide to Research Methods, 3,* 222-248.

Cohen, L. E., Kluegel, J. R., & Land, K. C. (1981). Social Inequality and Predatory Criminal Victimization: An Exposition and Test of a Formal Theory. *American Sociological Review, 46,* 505-524. https://doi.org/10.2307/2094935

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

Cole, T. (2022b). *Exploring Online Fraudsters' Decision-Making Processes*. Dissertation, Georgia State University.

De Keersmaecker, J., & Roets, A. (2020). All Victims Are Equally Innocent, but Some Are More Innocent than Others: The Role of Group Membership on Victim Blaming. *Current Psychology, 39,* 254-262. https://doi.org/10.1007/s12144-017-9763-9

Fong, C. (2020). Impact on Growing Diversity & Multi-Cultural Counseling at Work Place in Singapore: A Review. *Journal of Psychology & Psychotherepy, 10,* Article No. 369. https://doi.org/10.35248/2161-0487.20.10.369

Howell, C., Burruss, G., Maimon, D., & Sahani, S. (2019). Website Defacement and Routine Activities: Considering the Importance of Hackers' Valuations of Potential Targets. *Journal of Crime and Justice, 42,* 536-550. https://doi.org/10.1080/0735648X.2019.1691859

Hsu, J. W., & Willis, R. (2013). Dementia Risk and Financial Decision Making by Older Households: The Impact of Information. *Journal of Human Capital, 7,* 340-377. https://doi.org/10.1086/674105

Kaakinen, M., Keipi, T., Räsänen, P., & Oksanen, A. (2018). Cybercrime Victimization and Subjective Well-Being: An Examination of the Buffering Effect Hypothesis among Adolescents and Young Adults. *Cyberpsychology, Behavior, and Social Networking, 21,* 129-137. https://doi.org/10.1089/cyber.2016.0728

Lee, C. S. (2022). How Online Fraud Victims Are Targeted in China: A Crime Script Analysis of Baidu Tieba C2C Fraud. *Crime & Delinquency, 68,* 2529-2553. https://doi.org/10.1177/00111287211029862

Open AI (2023). *ChatGPT (18 october 2023) [Large Language Model].* https://chat.openai.com

Schaffer, D. (2012). The Language of Scam Spams: Linguistic Features of "Nigerian Fraud" Emails. *ETC: A Review of General Semantics, 69,* 157-179.

Stajano, F., & Wilson, P. (2011). Understanding Scam Victims. *Communications of the ACM, 54,* 70-75. https://doi.org/10.1145/1897852.1897872

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*. https://doi.org/10.1007/s12103-022-09706-4

Williams, E., Beardmore, A., & Joinson, A. (2017). Individual Differences in Susceptibility to Online Influence: A Theoretical Review. *Computers in Human Behavior, 72,* 412-421. https://doi.org/10.1016/j.chb.2017.03.002