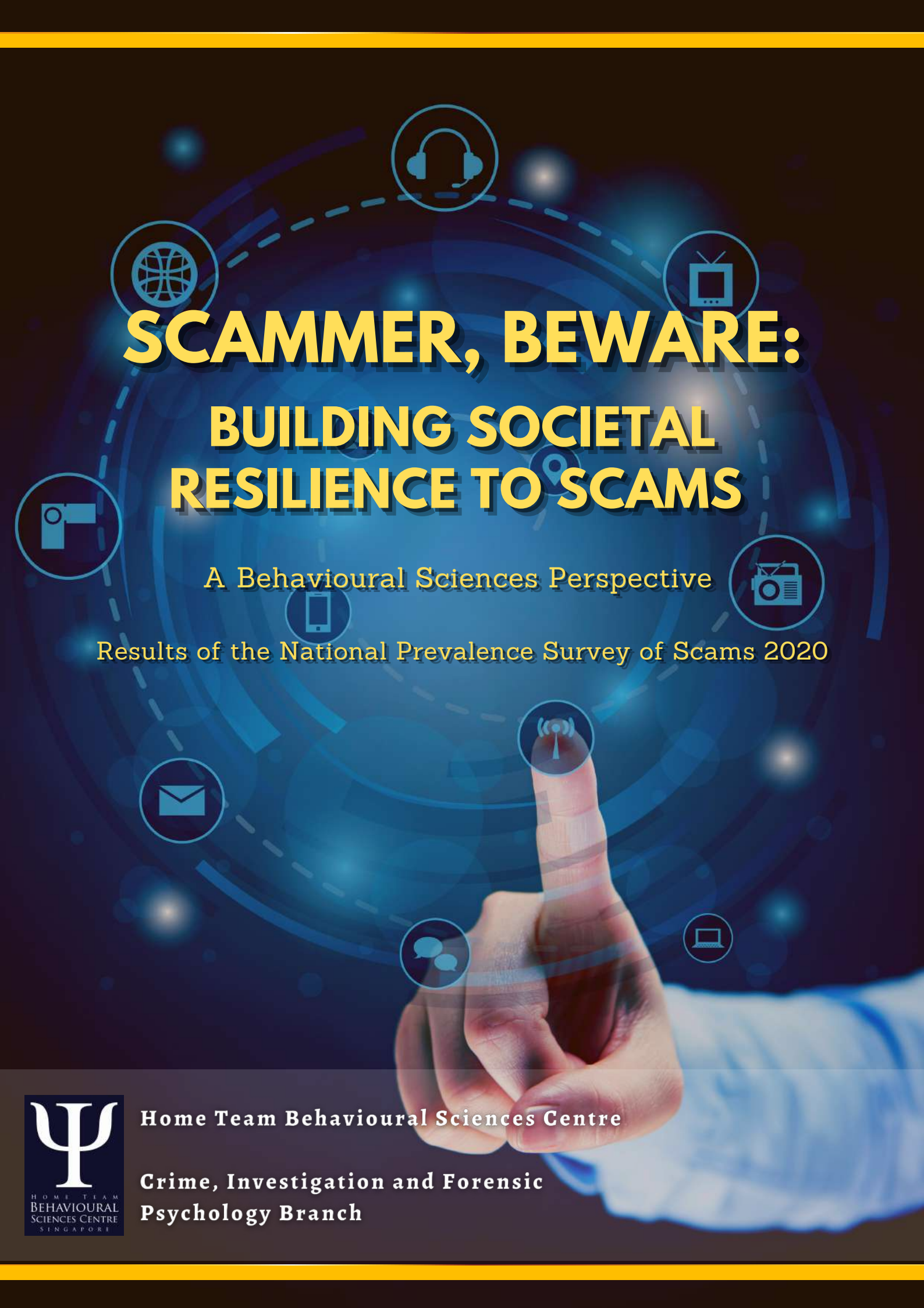


SCAMMER, BEWARE:

BUILDING SOCIETAL RESILIENCE TO SCAMS

A Behavioural Sciences Perspective

Results of the National Prevalence Survey of Scams 2020

Home Team Behavioural Sciences Centre

Crime, Investigation and Forensic Psychology Branch

CONTENT PAGE

FOREWORD 2

WELCOME MESSAGE 4

A NOTE ABOUT THE BOOK 5

EXECUTIVE SUMMARY 6

SCAMS ACROSS THE WORLD 8

THE SCAM LANDSCAPE IN SINGAPORE 16

THE BEHAVIOURAL AND PSYCHOLOGICAL ANALYSIS OF SCAMS 18

THE NATIONAL PREVALENCE SURVEY OF SCAMS 25

HOW INDIVIDUALS FALL PREY TO SCAMS 36

HOW TO AVOID SCAMS 49

A MULTI-PRONGED APPROACH TO SCAM PREVENTION 57

REFERENCES 64

ABOUT HTBSC 67

ACKNOWLEDGEMENTS 68

FOREWORD

Minister of State Mr Desmond Tan's Message

Scams are a grave issue. In the past five years, the number of reported scam cases and amount lost to scams have tripled.

In 2020 alone, scams accounted for 42% of all crime in Singapore with losses estimated at SGD 265 million. In 2021, the largest sum cheated in a single case of a China officials impersonation scam was SGD 6.2 million. Many victims have lost a large part of their retirement savings to scams.

But it is not just about monies lost. Victims of scams may become depressed, with some who even considered taking their life after falling victim to scams.

Government agencies, private industries and the community have to work together closely, to arrest the trend of rising number of scams. Since 2020, the government has set up the Inter-Ministry Committee of Scams (IMCS). The IMCS has different government agencies such as the Ministry of Home Affairs, the Singapore Police Force, the Cyber Security Agency of Singapore, the Infocomm Media Development Authority, the Ministry of Communications and Information, the Ministry of Trade and Industry, and the Monetary Authority of Singapore, to coordinate the Government's anti-scam efforts. We work with the private industry too.

The IMCS adopts a multi-pronged approach to tackle scams.

- **Strengthening enforcement.** We have set up specialised units in the Singapore Police Force (SPF) to disrupt scammers' operations, such as the E-Commerce Fraud Enforcement and Coordination Team to tackle e-commerce scams and the Anti-Scam Centre to serve as the nerve centre for investigations into scam-related crimes. The SPF has also stepped up collaboration and conducted joint operations with foreign law enforcement agencies to tackle transnational scams, through its Transnational Commercial Crime Task Force.

- **Partnering stakeholders to combat scams.** In addition to drawing on the expertise and resources across Government to combat scams, we also work closely with private sector stakeholders such as banks, digital platforms and telecommunications companies to disrupt scams. For example, SPF works with financial institutions to swiftly freeze bank accounts suspected to be involved in scammers' operations and to weed out money mules. SPF also established close working relationships with telecommunications companies to block spoof calls used by overseas scammers.

- **Public education.** We work with partners such as the National Crime Prevention Council to disseminate advisories through various media platforms, including messaging and social media platforms. We launched our anti-scam public education campaign, "*Spot the Signs. Stop the Crimes.*" in August 2020, focusing on sharing real-life scam examples to educate the public on how to spot the tell-tale signs of various scams.

The best defence against scams is a discerning and vigilant public. Everyone can play a part in stopping scams. Be alert and practice healthy scepticism. Help to raise awareness of scams by talking to your family and friends about scams.

To study the 'DNA' of scams so we disrupt them better, the MHA Home Team Behavioural Sciences Centre (HTBSC) conducted a large-scale research using the National Prevalence Survey of Scams in 2020. The survey yielded information about the behavioural and psychological profiles of scam victims and non-victims. Various inter-government agencies have adopted these findings captured in this report. We hope that this booklet, with its research findings, would be useful for your anti-scam efforts.

Mr Desmond Tan
Minister of State
Ministry of Home Affairs and Ministry of Sustainability and the Environment

WELCOME MESSAGE

It is with great pleasure that I introduce the '*Scammer, Beware: Building Societal Resilience to Scams*' to you. This book is the first of a series that seeks to shed light on the current scam landscape in Singapore.

Last year, led by the Office of Chief Psychologist, a working group was formed to comprehensively examine scams and the psychology of victims from multiple perspectives (i.e., victims, perpetrators, investigators, stakeholders and community).

Since its formation, we have taken on an active role in organising behavioural sciences research and psychological service resources in support of the ministry's anti-scam efforts and have been working closely with the Singapore Police Force and the Ministry of Home Affairs (MHA) Policy Development Division. In addition, we hope to create platforms and establish strategic links that enable us to leverage on the knowledge of our partners to provide solutions to current scam issues.

This book combines our current research and review on scams in recent times. Through this book, we hope to raise greater awareness of the current scam issues faced in Singapore. '*Scammer, Beware: Building Societal Resilience to Scams*' will highlight Singapore's latest scam prevalence rates and trends. In the last section of the book, we also hope to discuss preventing scam victimisation in our own backyard.

We hope this book will elucidate the importance of keeping safe from scams.

I look forward to sharing more findings in our forthcoming issues and wishing you an enjoyable read!

Dr Majeed Khader, Ph.D
Chief Psychologist
Office of Chief Psychologist
Concurrent Director Home Team Behavioural Sciences Centre

A NOTE ABOUT THE BOOK

To support the Home Team in its efforts to combat and manage scams, the HTBSC had conducted the National Prevalence Survey of Scams with the aim of obtaining a more comprehensive understanding of the scam situation in Singapore. This report describes the key findings obtained from the survey and draws links to the larger issues of why and how such global and local trends of scams perpetuate in the current security climate. It is also part of our existing efforts to raise greater public awareness on scam trends and prevention tips.

'*Scammer, Beware: Building Societal Resilience to Scams*' is the first of a series on scam prevalence and target profiles. It seeks to describe some demographic, behavioural and psychological characteristics that make individuals vulnerable to scam victimisation. Existing measures put in place to combat scams, and scam prevention tips for the public to adopt will also be shared in this issue.

We sincerely thank our Home Team partners (e.g., MHA Policy Development Division, Research & Statistics Division, Singapore Police Force), industry partners (e.g., Lazada, Shopee, Carousell, AXS Infocomm Pte Ltd, United Overseas Bank, DBS Bank, Oversea-Chinese Banking Corporation Limited) as well as academic partners (e.g., Nanyang Technological University, National University of Singapore, Singapore University of Social Sciences, James Cook University, Singapore Institute of Technology) for lending your expertise to our research.

As individuals, we can make a big difference by keeping ourselves updated on the latest scam trends, recognising signs of scams, and watching out for our loved ones against scams. To our readers, thank you for taking the time to read through this book. We hope that this book will serve as a general guide for all against scams.

Ms Whistine Chai Xiau Ting
Principal Psychologist / Senior Assistant Director
Crime, Investigation and Forensic Psychology Branch
Home Team Behavioural Sciences Centre

EXECUTIVE SUMMARY

Scams have been on the rise and cost the Singapore economy more than SGD 201 million in 2020 and continue to be a concern in 2021. These scam operations are organised to target human vulnerabilities and apply social influence techniques to prey on individuals. Scammers have set up scam operations all around the globe, such as in Australia, Canada, Hong Kong and the United States, and Singapore is no exception.

Based on the recent mid-year crime statistics released by the Singapore Police Force, it was reported that scams made up 43.2% of all reported crime cases, and was therefore a significant cause for the overall increase in number of reported crime cases in Singapore during the first half of 2021.

With the rising incidence of scams and financial losses in Singapore, coupled with an increase in the complexity of scam perpetration and the uncertainty experienced during a global pandemic, there is a growing interest and importance for us to enhance our methods in scam prevention and intervention. The increasing trend of scam cases also calls for a more scientific understanding of the scam situation in Singapore.

In order to get a better understanding of Singapore's scam landscape from the behavioural sciences and psychological perspective, the Home Team Behavioural Sciences Centre (HTBSC) recently conducted the National Prevalence Survey of Scams. This is the first of such studies conducted in Singapore with the aim of examining the prevalence rate of scam encounters and victimisation amongst Singapore Citizens and Permanent Residents. This survey sought to identify demographic, behavioural, and psychological characteristics that make individuals vulnerable to scam victimisation.

The survey found that seven in 100 Singaporeans fell prey to at least one scam over one year, between August 2019 to September 2020. It was also found that individuals were more prone to scam victimisation if they engaged in risky online activities, practised poor cyber hygiene, and endorsed unsecure online behaviours, indicating poor knowledge of safe cyber practices. Additionally, victims of scams also exhibited less vigilance, were more complacent and compliant, and adopted cultural attitudes that increased their susceptibility to scam victimisation.

In light of the pressing need to effectively control and curb scams in Singapore, it is recognised that concerted efforts by various stakeholders are necessary. The aim of this book is to 1) describe the findings from the National Prevalence Survey of Scams to vividly illustrate the scam situation in Singapore, and 2) highlight scam prevention and public education measures that Singapore has implemented in the fight against scams.

This report provides a more comprehensive understanding of the scam situation and victim profiles in Singapore. Additionally, the HTBSC hopes that it may serve as a starting point for greater discussion and study of this topic, as well as pave the way for many more outputs that can provide further insights for practitioners and policy-makers on anti-scam efforts.

1

SCAMS ACROSS THE WORLD

Most aspects of our lives have moved onto cyberspace. According to Johnson (2021), there were 4.66 billion active internet users around the world (which is approximately 59.5% of the global population) in January 2021. While the internet has brought multiple benefits, such as the ease of communication and access to an abundant amount of information, it is not without its pitfalls. Given the large number of active internet users today and how the Internet of Things (IoT) enables various internet-connected devices to interact and exchange information (Morgan, 2014), it is unsurprising that there is an excessive amount of personal data produced and stored online. As they trade privacy for convenience, internet users tend not to think about how much of their personal information is made available on the deep web, attracting cybercriminals to exploit the data-abundant cyberspace.

Cybercriminals refer to malicious users who profit from stealing company or personal data to commit acts of cybercrime using the internet and other technological systems and devices (Trend Micro, n.d.). Like how there are various types of crimes in the real world, there are also many crimes in the cyber world, such as malware and IoT hacking. In particular, the top cybercrime in 2020 globally was phishing scams (Zurier, 2016, as cited in BlueVoyant, 2020), which accounted for more than eight in 10 reported security incidents (Fruhlinger, 2020).

The phenomena of scams and fraud have been present in societies throughout history, with the concepts of cheating and fraudulent misrepresentation being ever-present in familiar colloquial references such as 'con-person', 'swindler', 'trickster', 'honey-trap', 'ponzi-scheme', and 'dishonest seller'. In an increasingly globalised and interconnected world, the opportunities and modes for interaction in societies have also evolved into new forms with the online space, new technologies, and new media.

CON-PERSON

SWINDLER

TRICKSTER

HONEY TRAP

PONZI-SCHEME

DISHONEST SELLER

Correspondingly, the perpetration of scams and fraud has also evolved into more borderless, sophisticated, and organised crimes, implying lowered barriers to scam offending and increased opportunities for scam victimisation.

Scams as Organised Crime

As highly organised and sophisticated borderless schemes, scam operations are becoming transnational and targeting a broader range of technological and human vulnerabilities. Scams pose a persistent global crime risk to individuals, organisations, enterprises, and countries alike as they exploit the online user interface with dark pattern techniques (Brignull, n.d.). For instance, they seek out potential human vulnerabilities by targeting our online behaviours (i.e., financial transactions, social media activities, shopping habits, internet use), and adapt social influence techniques to perpetrate their schemes (Button & Cross, 2017; Consumers International, 2019; European Consumer Centres Network [ECC-Net], 2017), demonstrating the premeditation and organisation of scam operations.

Some scammers also leverage on the operational flexibility of scams as perpetrators may set up mobile short-term 'rip and tear' scam operations (Shover et al., 2003) and even opt to diversify their operations to have cross-border elements (Levi, 2008), thereby reducing their likelihood of being met with enforcement actions.

The ensuing challenges of detecting and obtaining inter-jurisdiction prosecution that industry and law enforcement professionals would face due to the complexities of scams (Button et al., 2009; Button & Cross, 2017) mean that perpetrators may perceive a lowered risk of getting caught and prosecuted for their crimes, and may be emboldened further in their fraudulent criminal activities.

Notably, these challenges translate to a range of tangible impact as scams and fraud become increasingly endemic across societies, implicating many stakeholders, claiming many victims, and generating sizeable financial losses attributed to scams and fraud (International Public Sector Fraud, 2020). Moreover, on the individual level, scam victims may also experience intangible personal and psychological impacts (i.e., post-crime reactions and felt emotions). For instance, some victims may experience feelings such as self-blame, shame, anger, fear, sadness, and even engage in negative thinking patterns as they attempt to cope and make sense of their scam experience. Concurrently, victims may also encounter newly added life stressors (i.e., financial debt, relationship conflict, reduced mental well-being, and physical health) because of their scam experience (Button et al., 2012).

World Trends

There has been a rising trend in the prevalence of scams, making scams one of the top crimes around the world and a global crime concern. Critically, the world economy incurs an estimated cost of GBP 3.89 trillion (SGD 7.30 trillion) annually (Gee & Button, 2019). This section presents scam trends in different countries or cities based on various open-sourced reports. Note that these figures were obtained based on available scam reports around the world.

Australia

Based on available prevalence studies on scams, approximately 8.5% of Australians fell prey to scams and fraud between 2014 and 2015 (Australian Bureau of Statistics, 2016). Regarding re-victimisation rates in Australia, 28.8% of scam victims fell prey to scams more than once (Australian Bureau of Statistics, 2016). Approximately 61% of the most serious cases of scams were received via the Internet (including 39% by email, 7% by social media, and 15% by other ways over the Internet) (Australian Bureau of Statistics, 2016).

In 2020, an estimated 444,164 reports of scams and fraud added up to an estimated total monetary loss of AUD 850 million (SGD 858.6 million) experienced by victims (Australian Competition and Consumer Commission [ACCC], 2021), as compared to an estimated 167,797 reports of scams and fraud worth AUD 634 million (SGD 638.8 million) in 2019 (ACCC, 2020). The sharp increase observed was reportedly attributed to the **exploitation of crises** (i.e., Australian bushfires, and the global COVID-19 pandemic) by scammers (ACCC, 2021). Critically, these statistics were also estimated to reflect an under-reported figure (13%) of actual cases of scams and fraud (ACCC, 2021).

Trends in Australia

- 8.5% became a victim of scam between 2014 and 2015
- 28.8% of victims were repeat victims
- 61% of serious scam cases were encountered via the Internet
- Reported scam cases increased from 167,797 cases in 2019 to 444,164 cases in 2020
- Increase in scams is attributed to exploitation of crises (e.g., bushfires, pandemic)

Canada

In Canada, according to the Chartered Professional Accountants of Canada (CPA Canada) Annual Fraud Survey 2021, 73% of all respondents reported receiving fraudulent requests from at least one type of scam or fraud in their lifetime, and 33% of all respondents reported falling victim to at least one scam in their lifetime (CPA Canada, 2021).

Trends in Canada

- 73% received fraudulent requests
- 33% fell victim to at least one scam in their lifetime
- Reported cases of scams and fraud increased significantly from 46,465 cases in 2019 to 101,483 cases in 2020
- Reported numbers claimed to be under-representative of actual situation

Narrowing in on the year 2020, an estimated 101,483 incidents of scams and fraud were reported, amounting to an estimated total monetary loss of CAD 160 million (SGD 172.6 million) experienced by victims (Canadian Anti-Fraud Centre, 2021). The number of incidents and total monetary losses attributable to scams and fraud markedly increased as compared to the previous year in 2019.

In 2019, 46,465 incidents of scams and fraud were reported in Canada, amounting to an estimated total monetary loss of CAD 96.2 million (SGD 103.8 million) (Almazora, 2021; Canadian Anti-Fraud Centre, 2020). These reported numbers were claimed to be under-representative of the actual situation, with less than 5% of cases estimated to be reported to the authorities (Canadian Anti-Fraud Centre, 2021).

Europe

In Europe, according to a survey of 30 European countries (27 EU members, Iceland, Norway, and the United Kingdom), 56% of respondents experienced at least one fraud or scam over a period of two years between 2017 and 2019 (European Commission, 2020). In particular, only 21% of those who experienced a scam or fraud reported to an official authority, and the estimated average loss reported by those who experienced a scam or fraud was EUR 82 (SGD 131) in this survey (European Commission, 2020). Unsurprisingly, scams and fraud were similarly observed to be increasingly facilitated via online communication mediums (i.e., email, social media, online advertisements), apart from other traditional communication mediums such as phone calls (European Commission, 2020).

England and Wales

In England and Wales, the reported scams prevalence rate was estimated to be 6.6% in the year ending March 2020 (Office for National Statistics, 2020), and an estimated 822,276 reports of scams and fraud amounting to GBP 2.3 billion (SGD 4.3 billion) was reported to authorities between 2019 and 2020 (Action Fraud, 2020).

Trends in England and Wales

- 6.6% scam prevalence rate
- Number of fraud incidents increased significantly from 3.7 million cases between March 2019 and 2020 to 4.5 million cases between December 2019 and 2020
- 68% increase in remote banking fraud highlights the rise in number of individuals who turn to technology for daily activities

More recently, the estimated number of fraud incidents between March 2019 and 2020 was 3.7 million offences, with 12% of victims repeatedly falling prey to scams (Office for National Statistics, 2020). However, this number increased to 4.5 million offences when the Crime Survey for England and Wales (CSEW) was conducted between December 2019 and 2020 (Office for National Statistics, 2021).

Additionally, according to the findings from the CSEW, "2.9 million cases of fraud involving UK-issued payment cards, remote banking, and cheques" were reported by UK Finance in 2020 alone (Office for National Statistics, 2021). There was also a rise of 73,640 incidents (68%) in "remote banking" fraud during 2020, reflecting the rising number of individuals who are increasingly turning to technology to fulfil their day-to-day activities and how scammers are using this trend to their advantage (Office for National Statistics, 2021).

Hong Kong

In 2020, according to local crime statistics, there were an estimated 15,553 reported cases of deception (fraud) crime with approximately HKD 5.26 billion (SGD 920 million) lost to scammers, although an estimated HKD 3.07 billion (SGD 540 million) was intercepted by the Hong Kong police from victims locally and abroad (Hong Kong Police Force, 2021; Lo, 2021). Collectively, this comprises about HKD 8.33 billion (SGD 1.46 billion) of deceptive (fraud) crime proceeds laundered through Hong Kong bank accounts in 2020 alone (Hong Kong Police Force, 2021; Lo, 2021).

These statistics suggest a marked increase from 2019, where there were 8,216 reported cases of deception (fraud), with a comparable estimated HKD 3.039 billion (SGD 530 million) intercepted by Hong Kong police from all victims (Lo, 2020). Furthermore, it is also estimated that HKD 13 billion (SGD 2.27 billion) was involved in the five-year period from 2016 to 2020 (Hong Kong Police Force Security Bureau, 2021).

Trends in Hong Kong

- 15,553 reported cases of deception in 2020
- Marked increase in cases as compared to 8,216 reported cases in 2019
- Estimated SGD 920 million lost to scammers in 2020

The United States (U.S.)

Based on findings from the Federal Trade Commission's (FTC) Mass-Market Consumer Fraud Survey (Anderson, 2019), 15.9% of respondents reported being victims of one or more scams between 2016 and 2017. This represents approximately 40 million U.S. adult consumers. Based on the self-reported data from this survey conducted in the U.S., up to 54.5% of scam victims had fallen prey to more than one scam (Anderson, 2019), indicating a high rate of re-victimisation. In relation to monetary losses, the median loss recorded from these consumer frauds was USD 100 (SGD 135) in this survey (Anderson, 2019).

Trends in the U.S.

- 15.9% of Americans fell prey to at least one scam
- Up to 54.5% of victims were repeat victims
- More than half of respondents had encountered scams through the Internet
- Median loss increased from SGD 135 between 2016 and 2017 to SGD 421 in 2020

Referencing the recent year of 2020, separate self-reported data suggests the median loss for all fraud reports to be USD 311 (SGD 421) and that only an estimated 2.2 million fraud incidents were reported in 2020 (Federal Trade Commission, 2021).

However, we note that the above studies cited in this section were conducted in different periods, and utilised different measures and constructs, therefore the comparisons may not be as straightforward.

Rise in Scams Amidst the Pandemic

The pandemic-induced change from the usual way of everyday life may bring about various sources of added individual stress (Tan & Kurohi, 2020) as societies and individuals alike are posed the challenge of rapid adjustment to the new norms arising from the pandemic (i.e., expedited technological transformation, changes in social interactions). In addition, the presence of COVID-19 as an existential threat may mean individuals are fearful for their economic security, as well as the health and well-being of their loved ones (Baker et al., 2020; Mertens et al., 2020). Consequently, the challenge to adjust and make sense of an uncertain world can be stressful and challenging, such that individuals may experience negative emotions and anxieties, a hyper-vigilant state, and feel inclined to be harm-avoidant in response to a perceived threat from the new lifestyle changes (Taylor, 2019).

Interestingly, many COVID-19-related scams appear to recognise that the added stressors and change due to the pandemic result in individuals becoming more vulnerable targets for crime, as the improvised scam typologies hone in on these heightened emotional vulnerabilities and stressors to target the psychology of potential victims via their fraudulent schemes (Ma & McKinnon, 2021).

In fact, within these uncertain times, the emergence of COVID-19 variants of familiar and novel cybercrime and scams led to an even sharper increase in scams in the last two years. A predictable band of unscrupulous individuals - scammers and cybercriminals - has sought to turn these challenges into opportunities. While crimes involving more physical means have been on the decline (e.g., outrage of modesty cases), cybercrime and scams using virtual means have risen.

Over the past years, reports and advisories from reputable news channels, technology companies, as well as intelligence and enforcement agencies around the world have described new and recycled variants of scams or cybercrime that have surfaced with this outbreak (Chan et al., 2020; Levi & Smith, 2021).

These often appear in the form of impersonation scams, e-commerce scams, investment scams, fraudulent donations, phishing scams, malware attacks, and fake news relating to the pandemic (Interpol, 2020; You & Imran, 2020).

WHY IS THERE A RISE IN SCAMS AMIDST THE PANDEMIC?

Scammers recognise that the **added stressors** and **pandemic-induced changes** cause individuals to become more vulnerable and leverage on these vulnerabilities in their fraudulent schemes. These stressors and changes include:

Fear of Economic Insecurity

Concern for Health and Well-Being of Loved Ones

Expedited Technological Transformation

Changes in Social Interactions

As a result of Covid-19, there have been new and recycled variants of scams and cybercrime that have surfaced. These often appear in the form of:

Impersonation Scams

E-commerce Scams

Investment Scams

Fraudulent Donations

Phishing Scams

Malware Attacks

Fake News

2

THE SCAM LANDSCAPE IN SINGAPORE

While there are various types of cyber threats faced in Singapore, one that is increasingly prevalent and has commanded the nation's attention is scams, which have continuously claimed many individual Singaporeans as victims.

Although Singapore remains one of the safest cities in the world, it is not crime-free. In fact, as we focused on the fight against the COVID-19 pandemic, Singapore saw a significant rise in the number of cybercriminal activities in 2020, accounting for 43% of overall crime as compared to 26.8% in the previous year (Cyber Security Agency of Singapore [CSA], 2020; CSA, 2021). Despite scam cases that leverage on the pandemic being commonly reported in both global and local news, it is not the only type of cybercrime that prevails in Singapore.

In 2020, there were 89 incidents of ransomware which targeted various industries (e.g., manufacturing, retail, and healthcare), resulting in a concerning increase of 154% in ransomware cases as compared to 2019. About 47,000 unique phishing URLs were observed to be hosted on Singapore infrastructure in 2020 - comparable to the three-year record high of 47,500 URLs seen in 2019 (CSA, 2021). Additionally, the escalating use of command and control (C&C) servers as well as botnet drones seem to also be cyber threats that are of growing concern.

Of the various types of cyber threats faced in Singapore, scams have been increasingly prevalent. To illustrate, there was an 11.2% increase in the number of reported crimes in the first half of 2021 as a result of scams. In particular, scams made up a more significant proportion of all reported crimes in the first half of 2021 (43.2%) compared to the same period last year (40.0%) (Singapore Police Force [SPF], 2020; SPF, 2021a). When the analysis excluded the reported scam cases in Singapore, there was a 7.8% increase in crime cases reported in the first half of 2021 (Figure 1).

Narrowing in on scams, Singapore's top five scams of concern in 2021 include loan scams, e-commerce scams, investment scams, social media impersonation scams, and job scams (Figure 2), all of which constituted a large majority (68.9%) of the top ten scams reported in the first half of 2021.

In particular, the scam type with the largest number of cases was loan scams with a total of 1,243 cases, whilst the scam type with the highest total amount cheated was investment scams with an estimated SGD 66.2 million in financial losses. Although the total number of e-commerce scams saw a significant decrease in the first half of this year, investment scams and job scams recorded the third and fifth highest number of reported cases respectively amongst all scam types (SPF, 2021a).

Figure 1: Key statistics on reported overall Crime and Scams in Singapore (adapted from Singapore Police Force Facebook page, 2021)

The other scams that comprised Singapore's top ten scam types in the first half of 2021 include internet love scams, non-banking related phishing scams, banking-related phishing scams, credit-for-sex scams, and China officials impersonation scams (SPF, 2021a).

Figure 2: Key statistics on top scams of concern in Singapore (adapted from Singapore Police Force Facebook page, 2021)

3

THE BEHAVIOURAL AND PSYCHOLOGICAL ANALYSIS OF SCAMS

Effective scams operate and succeed on the basis of human vulnerabilities. Where potential victims of scams see a chance to get a good deal, build a connection, help someone in need, or make a quick buck, scam perpetrators see opportunities they can exploit.

Scammers are able to gain compliance by appealing to the psyche of their targets (i.e., convincing others of their sincerity, establishing credibility, or appearing as a means to an end at opportune times). To carry out their schemes, scammers make use of various **behavioural and persuasion tactics**, expressed through verbal cues, dynamic factors of their communication, and any supplementary aids (e.g., spoofed social media profiles, scam scripts, accomplices, etc.). These unscrupulous individuals carry out their schemes with varying degrees of consequences, with victims of scams suffering financial losses, emotional impacts, and even biopsychosocial effects (Button & Cross, 2017).

Scammers may adopt **social engineering tactics**, which refer to tactics that intend to trick or manipulate individuals into agreeing to take an action that does not benefit them, though in scam situations, it tends towards a loss (of information, money, trust, etc.). Through social engineering, individuals may end up clicking on fraudulent links, sharing personal details, or making payments or transactions without knowing that the action is part of a scam (Hadnagy, 2010). Social engineering tactics thrive due to decision-making errors inherent in us, which in turn lead to scam compliance (Fischer et al., 2013; Jakobsson, 2016; Lea et al., 2009).

Studies conducted by psychologists have found that when individuals adopt more emotion-based processing, they may end up making more errors and poor decisions. The **Elaboration Likelihood Model of Persuasion** (ELM) (Petty & Cacioppo, 1986) supports this finding as well (Figure 3). The ELM states that if a person is both **motivated and able** to process a message, they conduct deeper, effortful, and more logical processing (through the **central route**). Conversely, suppose the individual is **unmotivated or unable** to process a message, they may have more superficial, emotion-based processing (through the **peripheral route**), leading to quicker but poorer decision-making. Scammers aim to activate

this peripheral route (e.g., by applying time pressures) since targets are more susceptible to making mistakes and agreeing with deceitful scam requests through this route. Simultaneously, **other thinking errors or shortcuts** (e.g., optimism bias, confirmation bias, near-miss effect, sunk cost fallacy, fundamental attribution error) further sway targets away from rational thinking and towards complying with scammers (Haselton et al., 2015).[1, 2, 3, 4, 5]

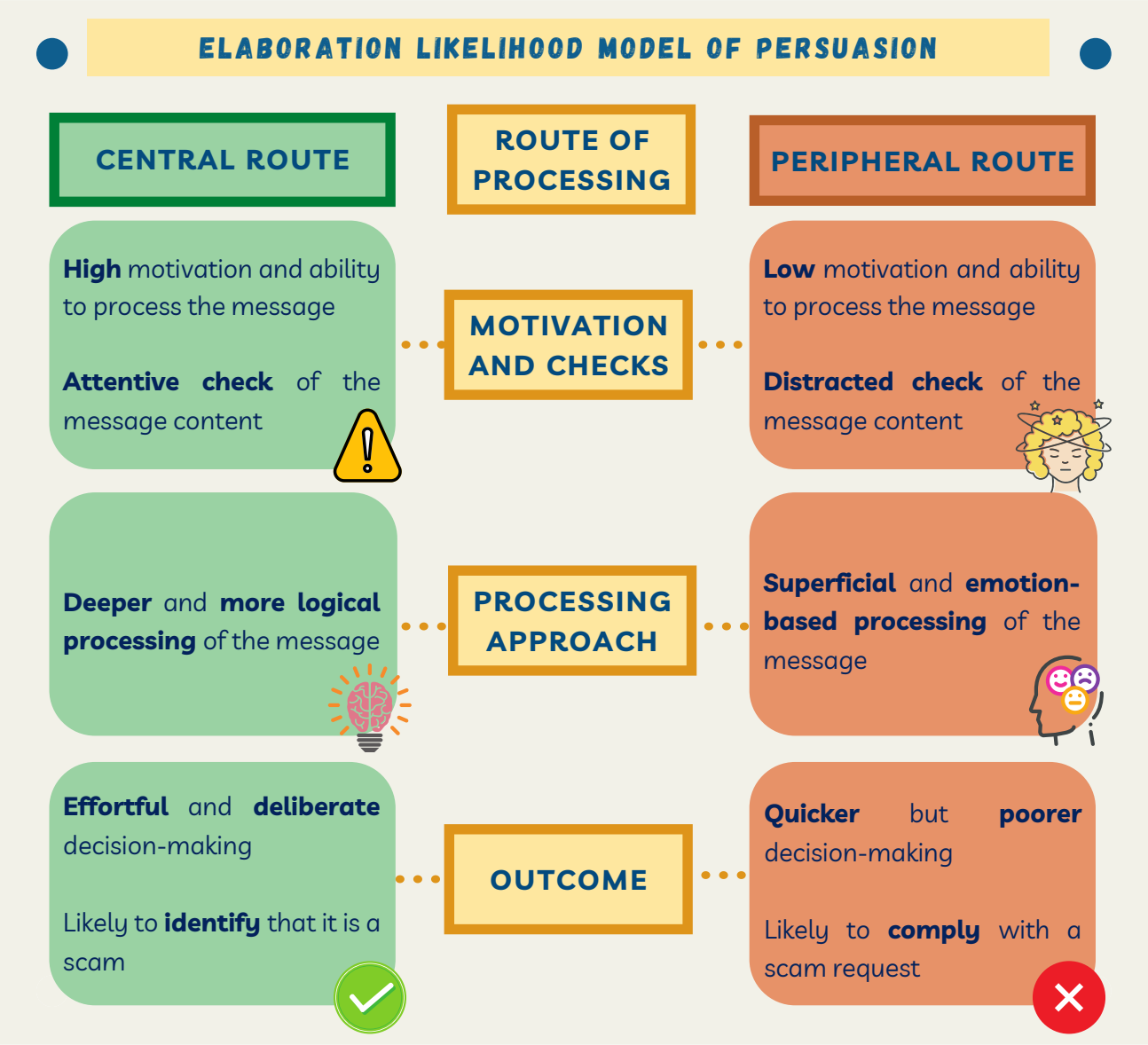


Figure 3: The Elaboration Likelihood Model of Persuasion (ELM)

[1] Optimism bias refers to the tendency to underestimate the likelihood of negative outcomes (here, scam victimisation) (Kirwan, Fullwood, & Rooney, 2018).

[2] Confirmation bias refers to the tendency to seek or interpret information that fits existing expectations or beliefs (Nickerson, 1998).

[3] Near-miss effect refers to the increased hope and expectation for future success after coming close to succeeding but actually failing to reach a goal (Reid, 1986).

[4] Sunk cost fallacy refers to heightened tendency to continue to participate in an endeavour due to the irrecoverable cost of prior investment of significant resources (e.g., time, money, effort) (Arkes & Blumer, 1985).

[5] Fundamental attribution error refers to the tendency for attributors to overestimate the role of dispositional (or personal) factors and underestimate the role of situational (or environmental) factors in judging the causes of behaviours or events (Ross, 1977).

The Persuasion Techniques

Altogether, the range of tactics used by scam perpetrators can be subsumed under three sub-categories: **victim selection techniques, perpetration strategies,** and **detection avoidance techniques** (Button et al., 2009; Norris et al., 2019). However, in dealing with the psychology of scams, and understanding why people fall victim to scams, it is important to focus on the perpetration tactics.

As per Cialdini (2001; 2016), there are seven **persuasion principles** which have been seen to efficaciously influence individuals. Namely, these persuasion principles are liking, social proof, reciprocity, commitment/consistency, authority, scarcity, and unity. Most of the scams, including the top scams of concern in Singapore, such as e-commerce scams, investment scams, loan scams, and social media impersonation scams, make use of these tactics to induce liking, establish credibility, develop a relationship, and/or create the illusion of dire circumstances that targets must act upon to avoid punishment or gain a reward. Table 1 details these persuasion principles alongside examples of their application in scam situations.

Persuasion Principle	Description	Example
Liking	Conveying high regard or fondness for the communicator	Scammers use compliments, affectionate terms, or other expressions of liking towards targets to foster likeability.
Social Proof	Using proof of peer support to convince the target to behave in a similar way	Job scammers add targets into a messaging group chat to show that others are yielding commission or income from the potential (fraudulent) deal.
Reciprocity	Providing a benefit in the hopes that the target will return the favour	Investment scammers offer potential victims an exclusive deal, hoping their generosity will convince targets to invest their money in the scam.
Commitment/ Consistency	Getting the target to commit actively, publicly, and voluntarily to a plan of action	Scammers get targets to agree that they will send the requested funds and convince them to follow through with the agreement.
Authority	Using details that purport expertise, credibility, and power to enforce behaviours	During the COVID-19 pandemic, scammers have made phone calls to potential victims, claiming to be a representative from the Ministry of Health.
Scarcity	Limiting the availability of desired benefits	E-commerce scammers entice targets to make a quick transaction before carefully analysing the details of the sale by providing a time limit on the discount of a product.
Unity	Drawing shared identities with the communicator	Romance scammers may highlight overlaps in ethnicity, religious affiliations or family background to build rapport with potential victims.

Table 1: The seven persuasion principles outlined by Cialdini (2001; 2016) with examples

Besides Cialdini's principles of persuasion, other tactics of social influence like the **foot-in-the-door technique** and the **door-in-the-face technique** may also be used to persuade people into ultimately falling victim to scams (Goldman, 1986). These techniques allow scammers to gain the confidence of their targets either by first making small, easy-to-fulfil requests to elicit compliance with larger ones in the future (foot-in-the-door) or make unreasonably large requests to get targets to comply with comparatively smaller (actual) requests later (door-in-the-face). Figure 4 and Figure 5 provide examples of how each of these techniques may be applied in a scam situation.

Figure 4: Example of foot-in-the-door scam technique

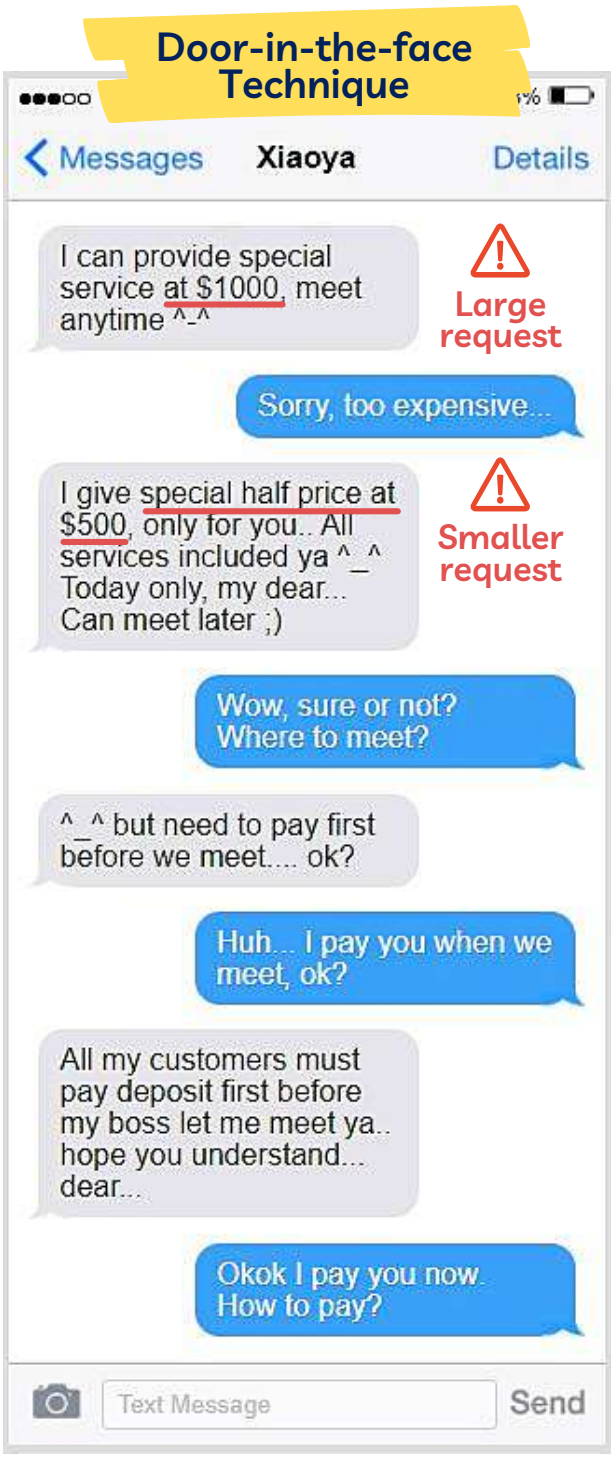


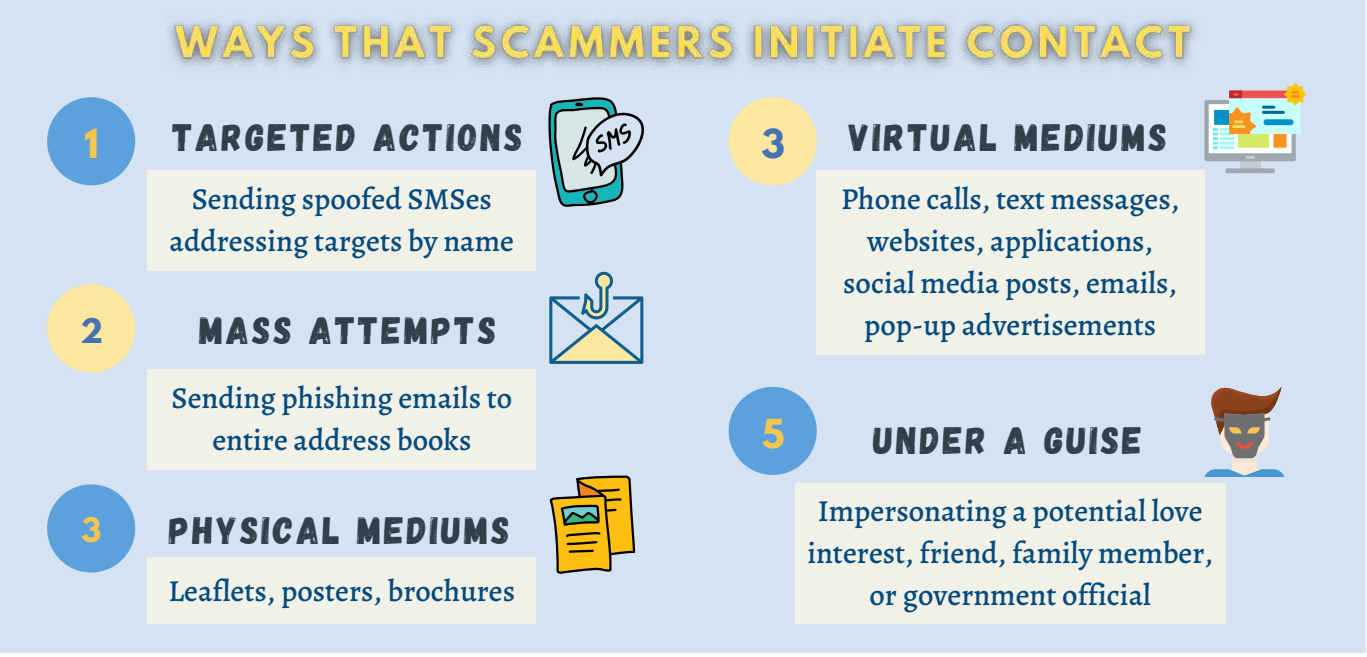
Figure 5: Example of door-in-the-face scam technique

The Scam Process

Looking at the broad progression of scams as a whole, most scams can be seen to begin with the initial point of contact between the scammer and the target, and followed through till the scam is either completed (e.g., the victim transfers money to the scammer) or disrupted (e.g., the target avoids falling for the scammer's claims and/or disengages).

Stage 1: Scammers Approach Their Target(s)

Scammers may use different modes, mediums, or platforms to initiate contact with their target(s). The scammer may use a number of lures to bring in potential victims, either via specifically targeted actions (e.g., by sending targeted spoofed SMSes addressing individuals by name) or mass attempts (e.g., by sending out mass phishing emails to entire address books). Additionally, a scammer may utilise virtual mediums (e.g., phone calls, text messages, websites, applications, social media posts, emails, pop-up advertisements) or physical mediums (e.g., leaflets, posters, brochures, notices). Furthermore, scammers may approach their target(s) under the guise of a potential love interest or confidante, the representative of a trustworthy organisation (e.g., loan provider from a recognised financial institution), impersonate an existing person (e.g., friend, family member, celebrity), or claim to be from a position of authority (e.g., Ministry of Health representative).



Stage 2: Scammers Persuade Their Target(s)

After initial contact is made, the scammer may adopt a dependable and trustworthy persona to convince their target and make requests that they would agree to. The scammer may do so via the seven persuasion principles (Table 1) mentioned earlier in this chapter. Moreover, some scammers also leverage local events (e.g., COVID-19 contact tracing efforts in Singapore) (Asokan, 2020) or make use of dialects (e.g., Singlish phrases) to appear more credible and convincing (Miranda, 2014).

Stage 3: Scammers Build Rapport & Establish Relationship with Their Target(s)

For some scams, particularly internet love scams or investment scams, the scammers may focus on the next stage: **rapport-building**. Rapport-building in this context refers to the (usually gradual) establishment of a relationship between the scammer and their target to create a **sense of shared understanding, attachment, and/or a basis for prolonged communication**. By creating a strong affiliation and leveraging the targets' innate needs, wants, or tendencies (e.g., appeals to greed, lust, safety, fear-avoidance, need for connection or love), scammers may be able to elicit irrational, emotion-based reactions instead of logical ones to reinforce compliance (i.e., via the aforementioned peripheral route of processing) (Yeo et al., 2020). In practice, scammers have been seen to exploit their targets' greed by claiming to provide quick financial returns on fraudulent investments, or appeal to one's innate fear-avoidant tendencies (e.g., via the use of forged proof that the target is in trouble with the law and the scammer could help the target avoid punishment).

Stage 4: Scammers Create Dependency with Their Target(s)

Once the relationship has been established, the scammer may **breed a sense of dependency**, before leading up to the **"hook"** or making a scam request. The scammer may do so by emphasising similarities between the target and themselves, displaying vulnerability, showcasing (fake) credentials, or offering access to exclusive opportunities. In some scams, especially internet love scams, **psychological grooming**, which refers to the psychological manipulation of individuals in order to elicit a high level of trust and dependency from the target (ABC News, 2017), could also be involved to entrap the victims in a cycle of victimisation. Through these efforts, the scammer may strengthen the shared relationship, making it easier to manipulate their target into believing a false claim and/or making a transaction. For instance, at this stage, if a scammer conveyed the urgent need for funds to cover medical expenses, an emotionally-invested target may agree to make the necessary transactions to help the scammer. In fact, the target may do so at a personal cost, in opposition to advice against such dealings, and even fall victim repeatedly.

Summary

Overall, basic human vulnerabilities and characteristics enable the success of social engineering techniques, applications of persuasion principles, and the general progression of scams. While individual-specific demographic characteristics, personality traits, knowledge, and skills may determine the extent to which people engage in a scam, other perpetration-oriented factors such as the mode and medium of approach, the use of dynamic factors, complementary tools, and other nuances serve as valid influences too.

Additionally, the methods and strategies employed by scammers may differ based on scam types; scams with different modus operandi employ different scam tactics and means of persuasion. Individuals may also fall victim to different tactics at different stages of scams. For example, fraudulent sellers in e-commerce scams may have more instrumental discussions (on quality and price of product, time of delivery, etc.) with buyers (potential victims). In contrast, scammers in internet love scams would likely reinforce greater emotional bonding with their targets. Nonetheless, the behavioural and psychological analyses of scams underline the commonalities amongst the scam experiences, both from the scammers' and (potential) victims' perspectives.

4

THE NATIONAL PREVALENCE SURVEY OF SCAMS (NPSS)

To support the Home Team (HT) in its efforts to combat and manage scams, a main working group comprising the Inter-Ministry Committee of Scams (IMCS) as well as their partnerships with the community and private sector stakeholders (i.e., banks, telcos, digital platforms) was established to aid in the fight against scams.

Aside from the main working group, the behavioural sciences aspect of scams was managed by a working group comprising psychologists and research analysts from the Home Team Behavioural Sciences Centre (HTBSC) and Police Psychological Services Department (PPSD). Together, this working group sought to comprehensively examine scams from various perspectives (i.e., victims, perpetrators, investigators, stakeholders and community), with an emphasis on the behavioural and psychological mechanism of scams.

HTBSC had recently conducted the NPSS to obtain a more comprehensive understanding of the scam situation in Singapore. The NPSS, the first of such studies in Singapore, was conducted to examine the prevalence rate of scam encounters and victimisation amongst Singapore Citizens and Permanent Residents.

Apart from identifying demographic, behavioural, and psychological characteristics that make individuals vulnerable to scam victimisation, this survey also looked into the public's perception towards our scam prevention efforts.

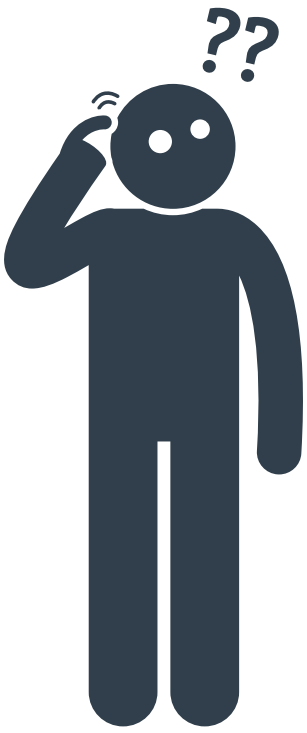
Research Aim

The study was primarily interested in identifying the characteristics of those who are prone to scams and those who have not been victimised. For example, what type of habits, characteristics, and behaviours did victims exhibit that made them more prone to falling prey to scams? On the other hand, what traits, characteristics and attitudes did non-victims display that may have protected them from scam victimisation?

What habits, characteristics, and behaviours did the victim exhibit that made them more susceptible to scams?

What traits, characteristics, and attitudes did non-victims display that may have protected them from scams?

WHAT CAN WE LEARN FROM BOTH THE VICTIMS AND NON-VICTIMS TO AID IN SCAM PREVENTION?



The NPSS sought to provide HT with a better understanding of the scam prevalence and situation in Singapore. This would, therefore, assist in the formulation of coherent scam prevention education strategies to reduce scam rates in Singapore.

Figure 6: Infographic about the National Prevalence Survey of Scams

Components of Study

In order to examine the scam situation in Singapore as well as to comprehend the victim profiles extensively, the survey was conducted in two phases.

Phase 1A Quantitative Analysis: Internet Survey

- National Prevalence Survey of Scams (N = 4043)
  - Singapore Citizens and Permanent Residents
- Booster Sample: Age 20 - 29, Indian Singapore Citizens and Permanent Residents, Malay Singapore Citizens and Permanent Residents, Students
- Fieldwork Period: 17th August 2020 to 28th September 2020

Phase 1B Quantitative Analysis: Internet Survey

- In-depth analysis of top scams of concern:
  - E-commerce Scams
  - Loan Scams
  - Investment Scams
  - Social Media Impersonation Scams

Preliminary Analysis

Literature Review of Research and Survey on Scams

To develop the survey items, an intensive literature review of close to 200 international and local journal articles on scams and fraud was conducted. In addition, surveys on scams and fraud conducted by international government agencies and public organisations were studied and used as a benchmark against the research conducted in Singapore. This in-depth review of the existing literature revealed insights into the worldwide prevalence rate of scams, the trends and impact of scams and fraud, as well as the underlying risk and protective factors of scam victimisation.

Consultation Sessions with Academic Practitioners; Pre-sensing Survey on Underlying Factors Associated with Scams

Taking cultural and localised issues into context, the research team had also conducted a pre-sensing survey to explore the various factors that may have contributed to individuals becoming victims of scams. Combining factors and themes that emerged from the preliminary analysis, a questionnaire comprising of demographic, psychological and behavioural variables was formulated. In order to ensure that the variables were relevant and applicable, a series of consultation sessions were conducted with HT officers dealing with scams, and academic partners who have vast research experience and expertise.[6] Findings obtained from the in-depth literature review, the pre-sensing survey, and consultation sessions were useful in informing the development of the survey items.

Survey Design

Measures

The survey comprised four sections measuring 85 variables. Apart from demographic factors, questions relating to respondents' scam experiences were asked. Survey questions were also developed to examine respondents' perceptions of Singapore's current scam prevention efforts and policies. Subsequent sections of the survey included areas such as respondents' attitudes and behaviours that might have impacted their vulnerability. Based on an extensive review of the literature and risk and protective factors of scam victimisation, these areas were examined and selected with regard to their potential in shaping current and future scam prevention and intervention strategies. The following areas were included in the NPSS:

[6] Contributors include Home Team partners (i.e., Singapore Police Force, Research and Statistics Division, Home Team Behavioural Sciences Centre, Police Psychological Services Department), e-commerce platforms (i.e., Lazada, Carousell, AXS, Alipay), local banks (i.e., United Overseas Bank, DBS Bank, OCBC Bank) and Institutes of Higher Learning (i.e., Nanyang Technological University, National University of Singapore, Singapore University of Social Sciences, Singapore Institute of Technology, James Cook University, and University of Reading Malaysia). The academics consulted include Associate Professor Fred Long Foo Yee, Mr Ong Kian Chye, Assistant Professor Jiow Hee Jhee, Dr Natalie Pang Lee San, Dr Razwana Begum, Dr Emily Ortega, Associate Professor Denise Dillion, Associate Professor Jonathan Ramsay, Dr Chung Kai Li, Assistant Professor Olivia Choy, Associate Professor Krishna Savani, and Associate Professor Elmie Nekmat.

DEMOGRAPHIC FACTORS

- Age
- Occupation
- Education
- Employment
- Nationality
- Citizenship
- Housing Type

SCAM AWARENESS & EXPERIENCES

- Scam prevalence in the past year
- Lifetime scam prevalence
- Motivations of victimisation
- Awareness & opinions of scam prevention efforts
- Guardianship & follow-up actions
- Remediation experience & loss recovery
- Awareness & opinions of existing policy interventions

KNOWLEDGE & USAGE

- Online activities
- Cyber-hygiene practices
- Financial literacy
- Vigilance on scams
- Complacency
- Knowledge of scam tactics
- Attitudes towards sharing personal information

Some of the survey questions relating to respondents' knowledge and online usage factors influencing scam vulnerability were adapted from international studies on online scams, such as the 'Survey on Risk Factors that may Lead to Becoming an Internet Fraud Victim' conducted by the American Association of Retired Persons (AARP; Shadel et al., 2014).

Questions on personal factors were adapted from several validated psychometric scales, namely, the Susceptibility to Fraud Scale (STFS), the Short Urgency, Premeditation, Perseverance, Sensation Seeking, Positive Urgency, Impulsive Behaviour Scale (SUPPS-P) and the Contingencies of Self-Worth Scale.

PERSONAL FACTORS

- Cultural Attitudes
- Impulsivity
- Compliance
- Self-esteem

Procedures

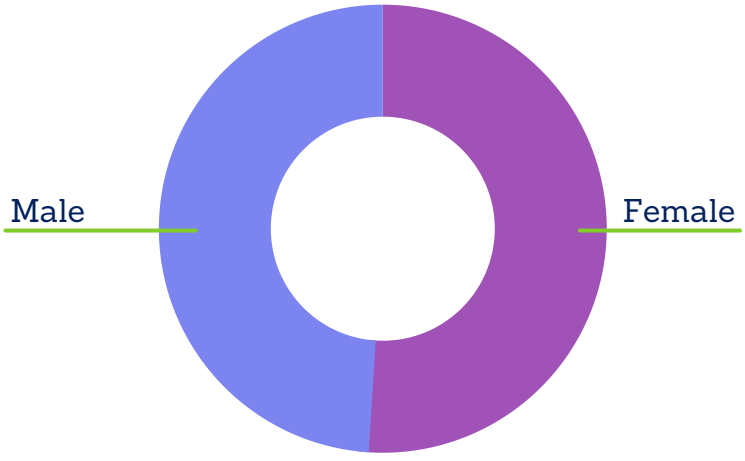
Working with an established survey company, this study saw a total of 4,043 Singapore Citizens and Permanent Residents who participated in the survey via an online platform. Participants shared their scam experiences, perception of scam prevention initiatives, and attitudes and behaviours that might have an impact on scam vulnerability. Participants took approximately 40 minutes to complete the survey.

To ensure survey findings could be generalisable to the Singapore population, the sample was stratified according to Singapore's demographic variables such as age, gender, ethnicity, region, and dwelling types. The data was further weighted to correct biases in the survey sample, such as over-representation or under-representation of specific groups, by taking population differences into account. The survey respondents were further categorised into five groups of interest: One-Time Victims, Repeat Victims, Near-Misses, and Evaders (refer to Figure 6 for more details) as well as the Non-Hit group (i.e., those who had not been approached by scammers during the one-year period that the survey was conducted).

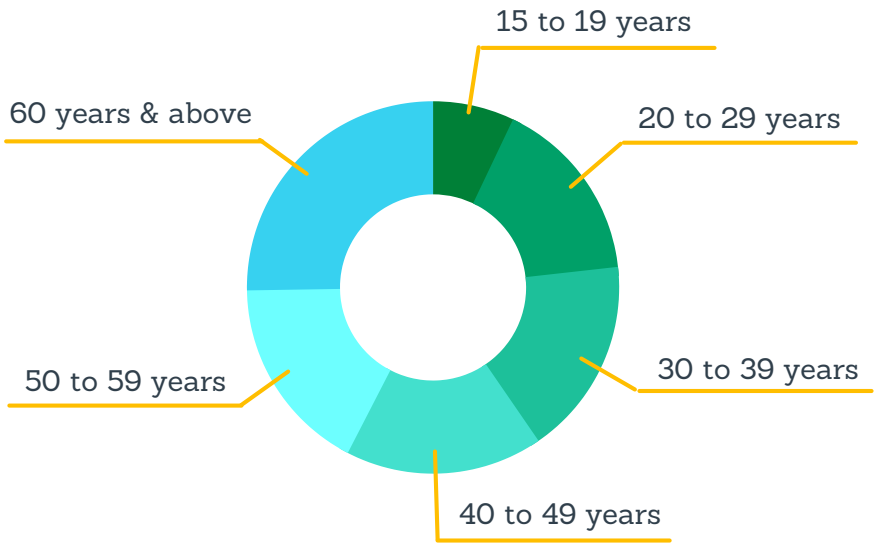
Besides the analysis of descriptive statistics for demographic variables, significant testing was conducted to derive results from the NPSS, which will be further discussed in this book.

Demographics of Survey Respondents

The demographic breakdown of respondents are as follows:

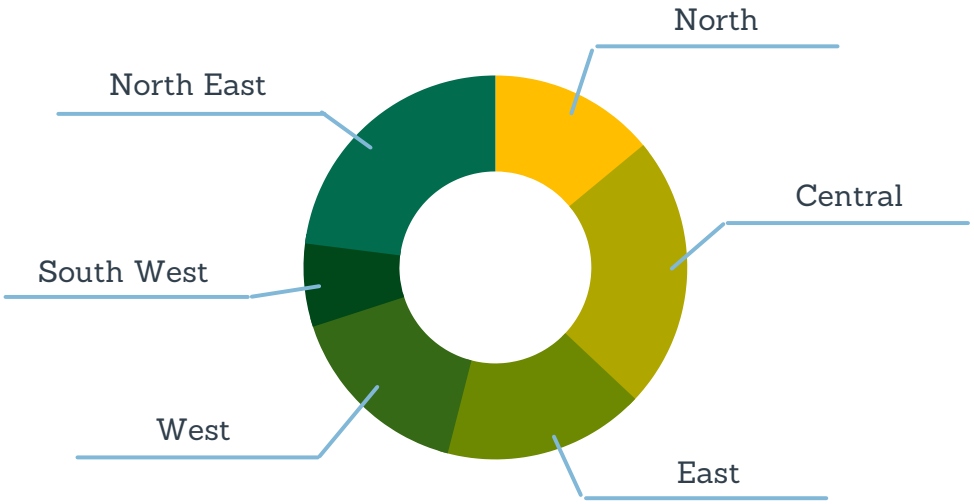


Respondents comprised 49% who were male and 51% who were female.



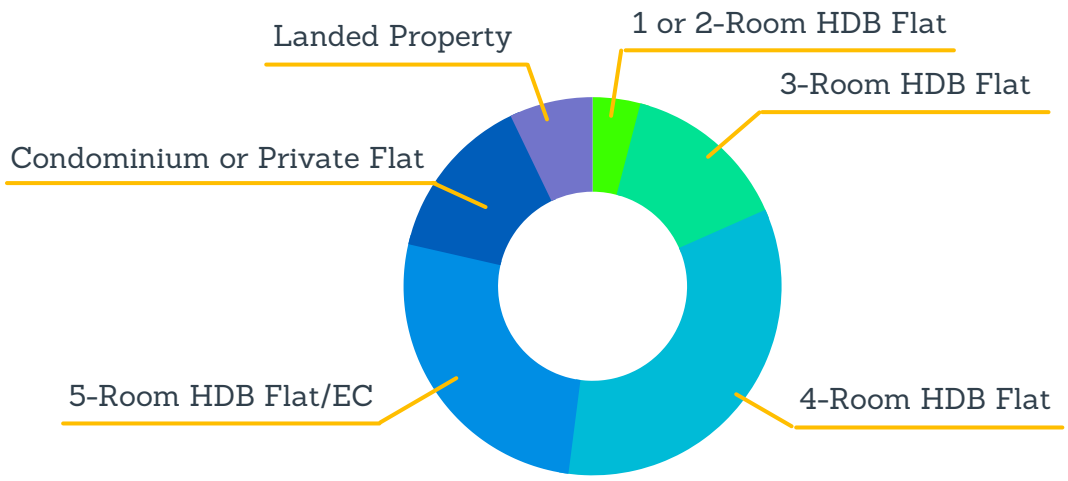
Respondents comprised individuals from six different age groups:

- 7% were between 15 to 19 years
- 16% were between 20 to 29 years
- 17% were between 30 to 39 years
- 17% were between 40 to 49 years
- 17% were between 50 to 59 years
- 25% were 60 years of age & above



Respondents from this survey lived in different regions in Singapore:

- 14% lived in the North region
- 23% lived in the Central region
- 17% lived in the East region
- 16% lived in the West region
- 7% lived in the South West region
- 23% lived in the North East region



Lastly, respondents from this survey lived in different types of housing:

- 4% lived in a 1 or 2-room HDB flat
- 14% lived in a 3-room HDB flat
- 33% lived in a 4-room HDB flat
- 26% lived in a 5-room HDB flat/EC
- 14% lived in a condominium or private flat
- 7% lived in a landed property

Scamming Singaporeans: How Many Fell Prey?

Although scam cases are drastically rising, many are unaware of the exact prevalence rate of scams in Singapore. Findings from the NPSS vastly illustrates the local scam landscape.

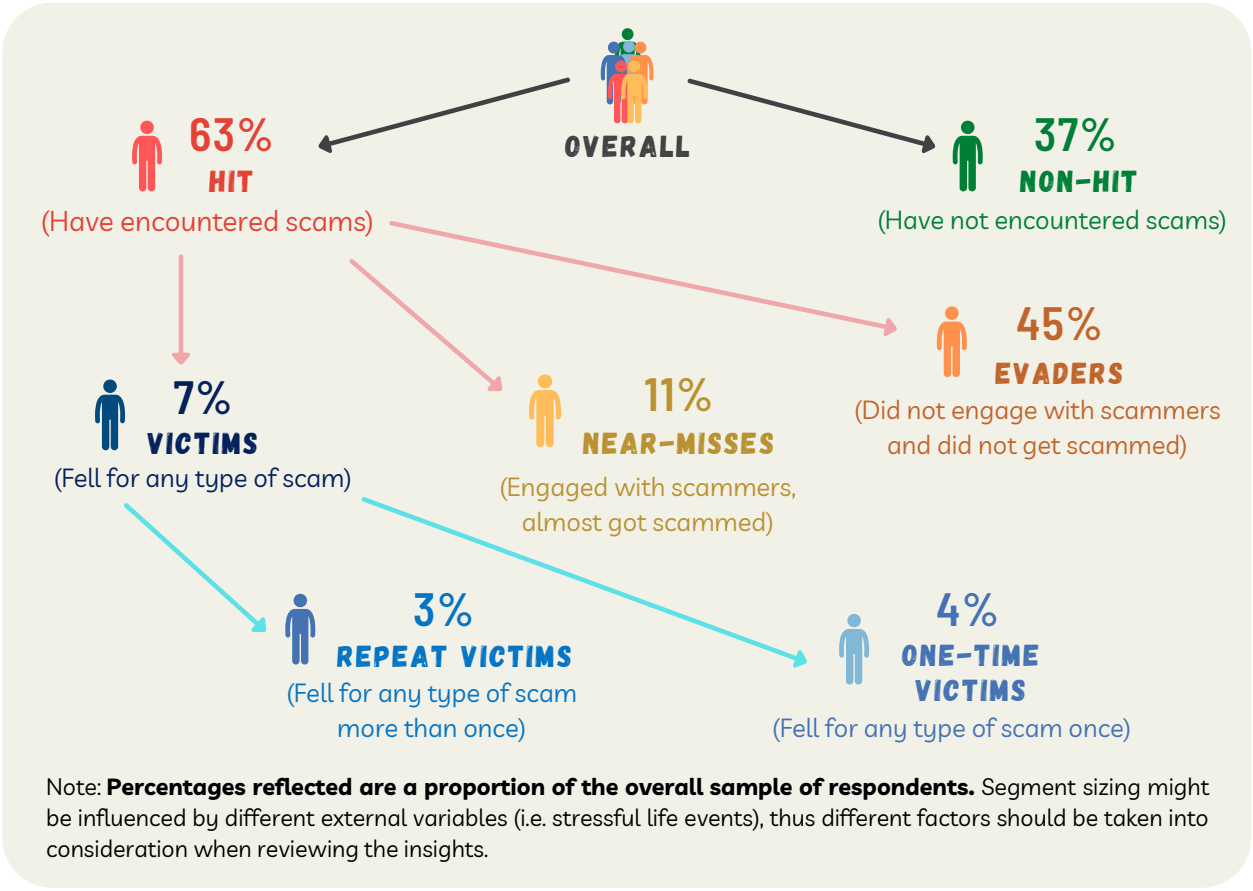


Figure 7: Statistics on the prevalence rate of scams in Singapore, based on the National Prevalence Survey of Scams

Over the last year (i.e., from August 2019 to September 2020), the survey found that of the total respondents, approximately six in 10 (63%) respondents had encountered scams, suggesting that the prevalence and occurrence of scams in Singapore is high. 45% of overall respondents successfully evaded falling prey to the scammers, and 11% engaged with the scammers but were a near-miss (i.e., almost got scammed). More importantly, the prevalence rate of scam victimisation in Singapore is seven in 100 respondents, which is equivalent to an estimated 300,000 individuals in the Singaporean and Permanent Resident (PR) population. Out of the overall respondents, it was found that while 4% fell prey to scams only once, 3% of respondents were repeat victims and fell prey to scams at least twice (Figure 7).

Scam Encounter Frequency

Overall, respondents reported encountering an average of 3.17 scams per month. Notably, victims reported a higher frequency of scam encounters than near-misses and evaders. Specifically, repeat victims reported the highest average number of scam encounters of **7.16 scams per month**.

Overall	Victims	Near-Misses	Evaders
			
3.17 scam encounters per month	5.18 scam encounters per month	3.49 scam encounters per month	2.76 scam encounters per month

The survey also found that scams were often encountered through online channels such as internet websites, online advertisements, and short-message services (SMS).

An average of 3.77 scams are encountered through internet websites per month

An average of 3.77 scams are encountered through online advertisements per month

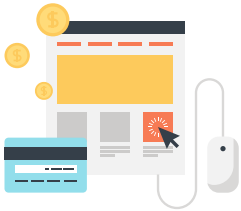
An average of 3.45 scams are encountered through SMS per month

Types of Scams Most Commonly Encountered

Subsequently, the NPSS identified that victims had more frequently fallen prey to a particular type of scam in the past year, with 31% of respondents falling prey to **e-commerce scams**. Some of the other scams that had been commonly encountered include investment scams (16%), loan scams (15%), and social media impersonation scams (15%). The different types of scams are described below.

E-commerce Scams

- Goods and services purchased online were fake goods, incorrect goods, or were never received



Investment Scams

- Scammers offer a false investment opportunity for which payment is made, but no returns are delivered

Loan Scams

- Loans that are offered to targets require an upfront admin fee. Following the payment of admin fee, the offered loan is not delivered

Social Media Impersonation Scams

- A compromised or spoofed social media account is used to pose as friends or family members to mislead targets and eventually ask for money

This chapter has elaborated on the purpose of the NPSS and provided a brief description of the prevalence rate of scams. The next chapter will describe the profile of victims in Singapore in an effort to better understand the demographics, mindsets and beliefs, and behaviours that increase one's susceptibility to scam victimisation.

5

HOW INDIVIDUALS FALL PREY TO SCAMS

Who Are The Scam Victims?: Demographic Insights

Victims in this chapter refer to individuals who have fallen for any type of scam in the past year. In Singapore, it was found that seven in 100 of the Singaporean Citizen and Permanent Resident population had become victims of any type of scam in the past one year and that the average monetary loss per victim was estimated to be SGD 37,227. Of this victim pool, respondents were further divided into two groups - one-time victims and repeat victims. The results from the NPSS suggest that over the past year, 163 respondents (4%) were one-time victims and the average monetary loss incurred by one-time victims was found to be approximately SGD 3,966 (Figure 8).

Figure 8: Average monetary loss of general victims, one-time victims and repeat victims

On the other hand, repeat victims comprised a total of 134 respondents (3%) over the past year. Despite the seemingly small percentage of repeat victims recorded in the overall sample of respondents, we found that **approximately one in two victims (45%) had fallen prey to more than one scam** over the past year. Moreover, repeat victims were found to have suffered an average monetary loss of SGD 74,200, which is almost 19 times higher than the average monetary loss incurred by one-time victims (Figure 8).

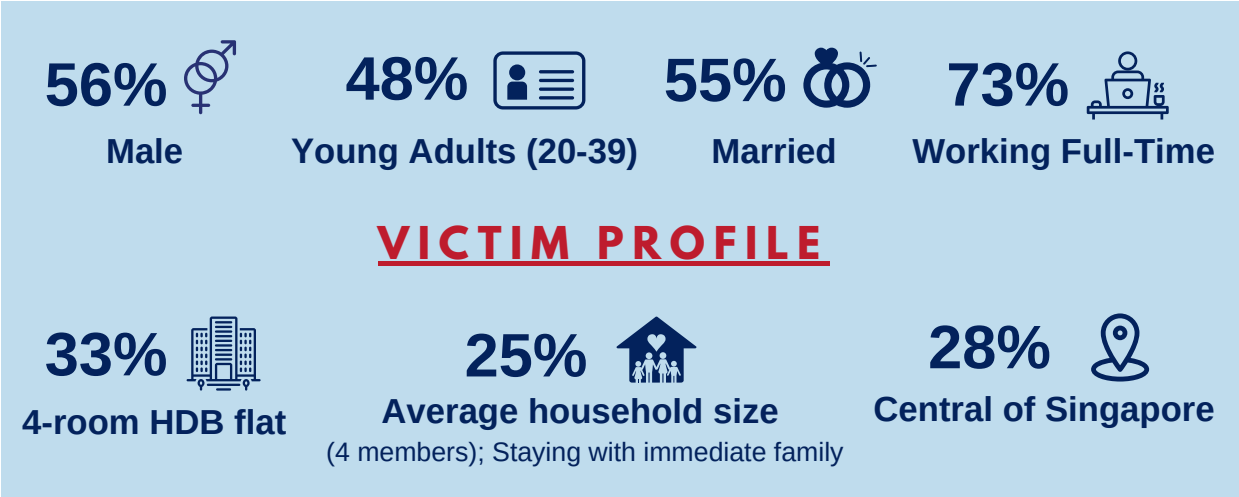
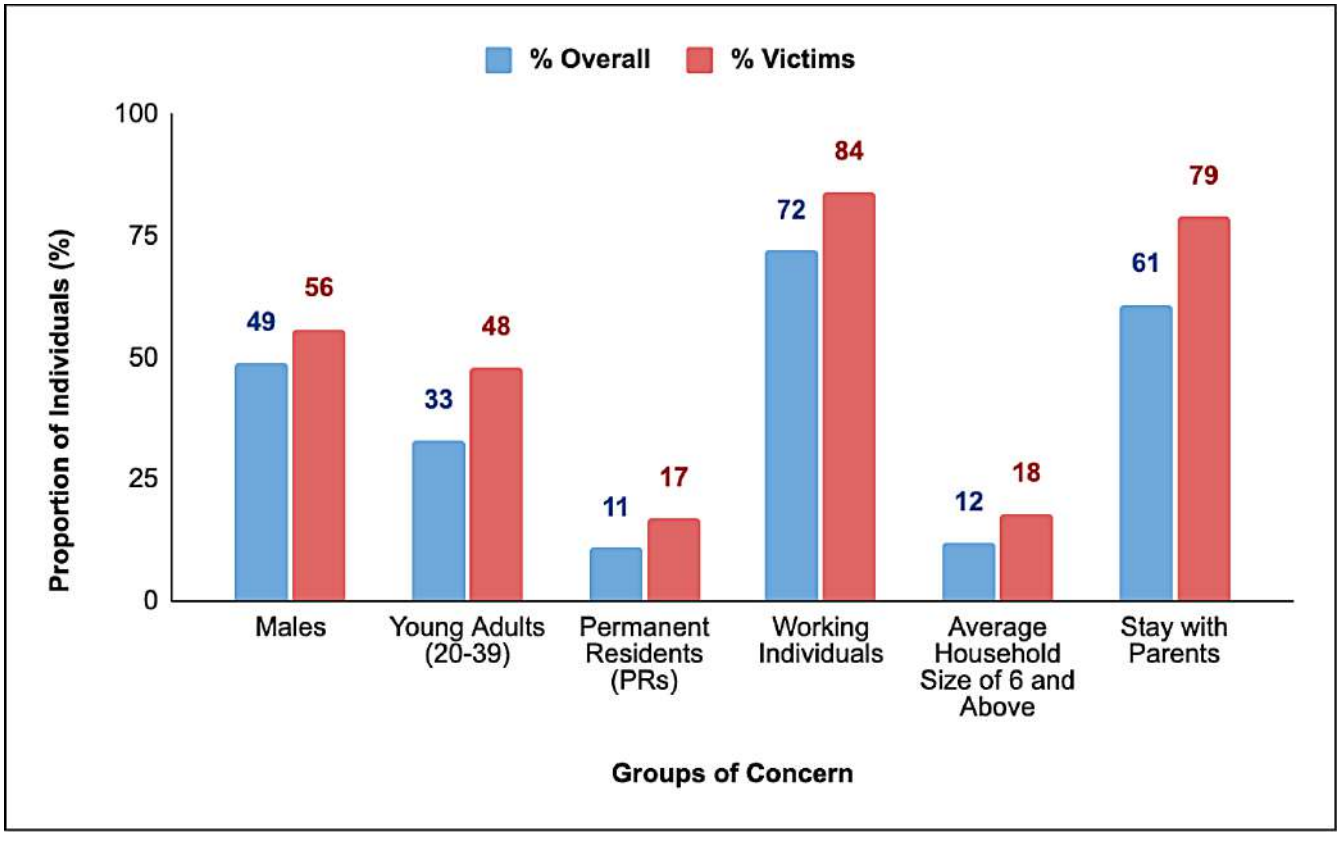


Figure 9: Demographic profile of victims

Examining the demographic profile of victims (n = 297), the survey found that most respondents who had previously been a victim of scam tended to be males, between the age of 20-39, married, working full-time, live in a 4-room HDB flat, live in central Singapore, and stay with their immediate family (Figure 9). Despite deriving this victim profile from the survey findings, it is not an implication that an individual who does not fall into this victim profile is safe from scam victimisation, and vice versa. Anyone can be a potential scam victim, but this victim profile highlights groups who have shown a higher tendency of falling prey to scams.



Note: The differences between % Overall and % Victims are significant at $p < .05$.

Figure 10: Groups of concern among victims

Separately, this study further examined if any groups were more vulnerable to becoming scam victims. This was done by comparing the overall sample population with the victim pool to identify groups that were over-represented among the victims. For example, the survey identified young adults between the age of 20 to 39 as a **group of concern** as they comprised 48% of the victim pool, even though they only constituted 33% of overall respondents, and hence were over-represented in the victim pool.

We found that males, individuals aged 20 to 39 years old, Permanent Residents, working individuals, those living in large households, and those staying with their parents were over-represented. In other words, these groups of individuals were more vulnerable to falling prey to scams. Figure 10 highlights the various groups of concerns among victims.

What Are Their Online Habits?: Behavioural Insights

Besides investigating their demographic profile, the online usage and activities of respondents were also examined to better understand users' habits and experiences. Generally, Singaporeans spend a substantial amount of time (approximately six hours per day) online on different kinds of activities. Figure 11 illustrates the different types of online activities that respondents reportedly engage in at least once a week.

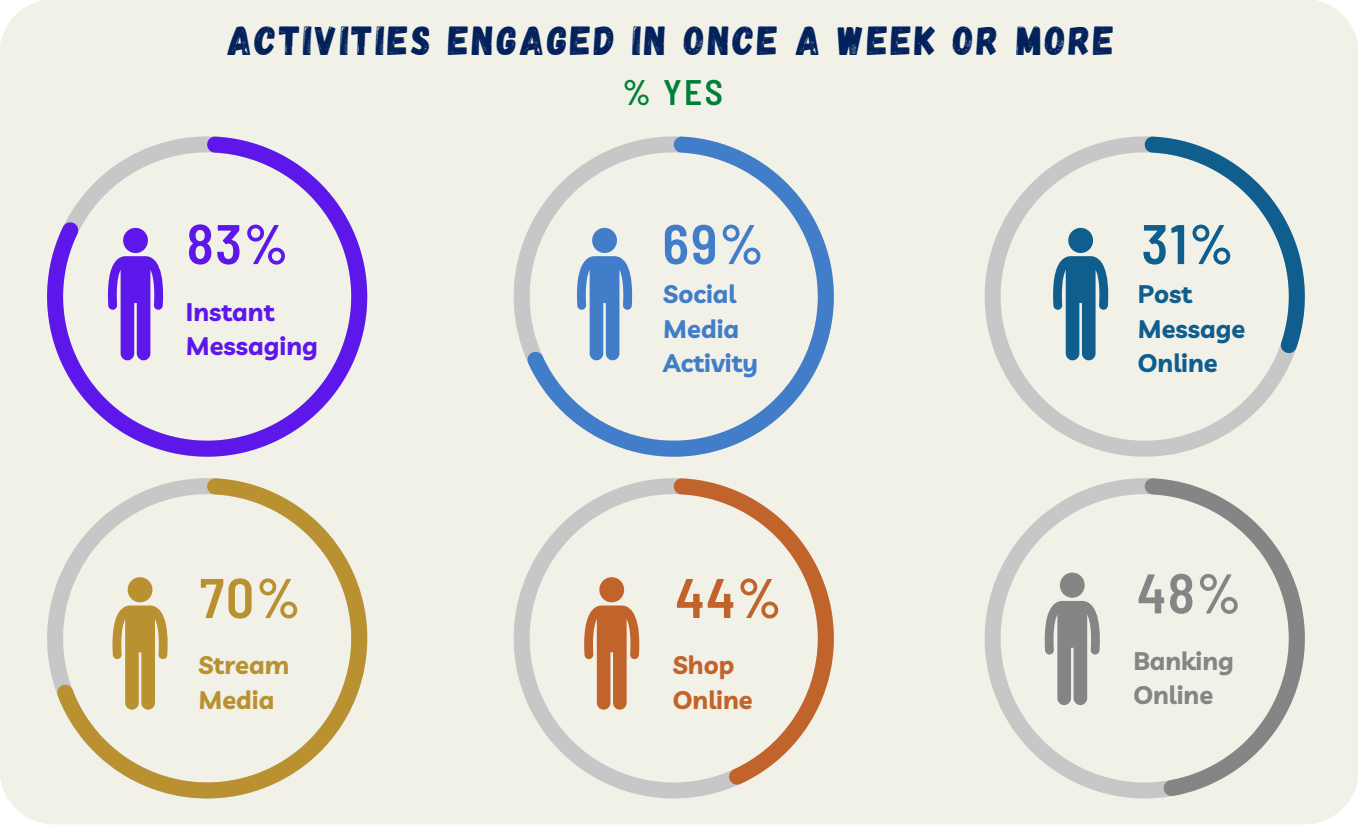


Figure 11: Different kinds of online activities respondents engaged in at least once a week

After further analysis, the researchers of the study found that all groups of respondents - victims, near-misses, and evaders - spent approximately the same amount of time online. So, why do victims fall prey to scams but evaders do not?

Type of Online Activities

Intriguingly, it is the **type of online activities**, rather than the amount of time spent online, that may increase one's risk of falling prey to scams. Victims spent a larger proportion of their time online engaging in more risky online behaviours, such as online shopping, making online transactions, and downloading files online (Figure 12), causing them to be more vulnerable to scams.

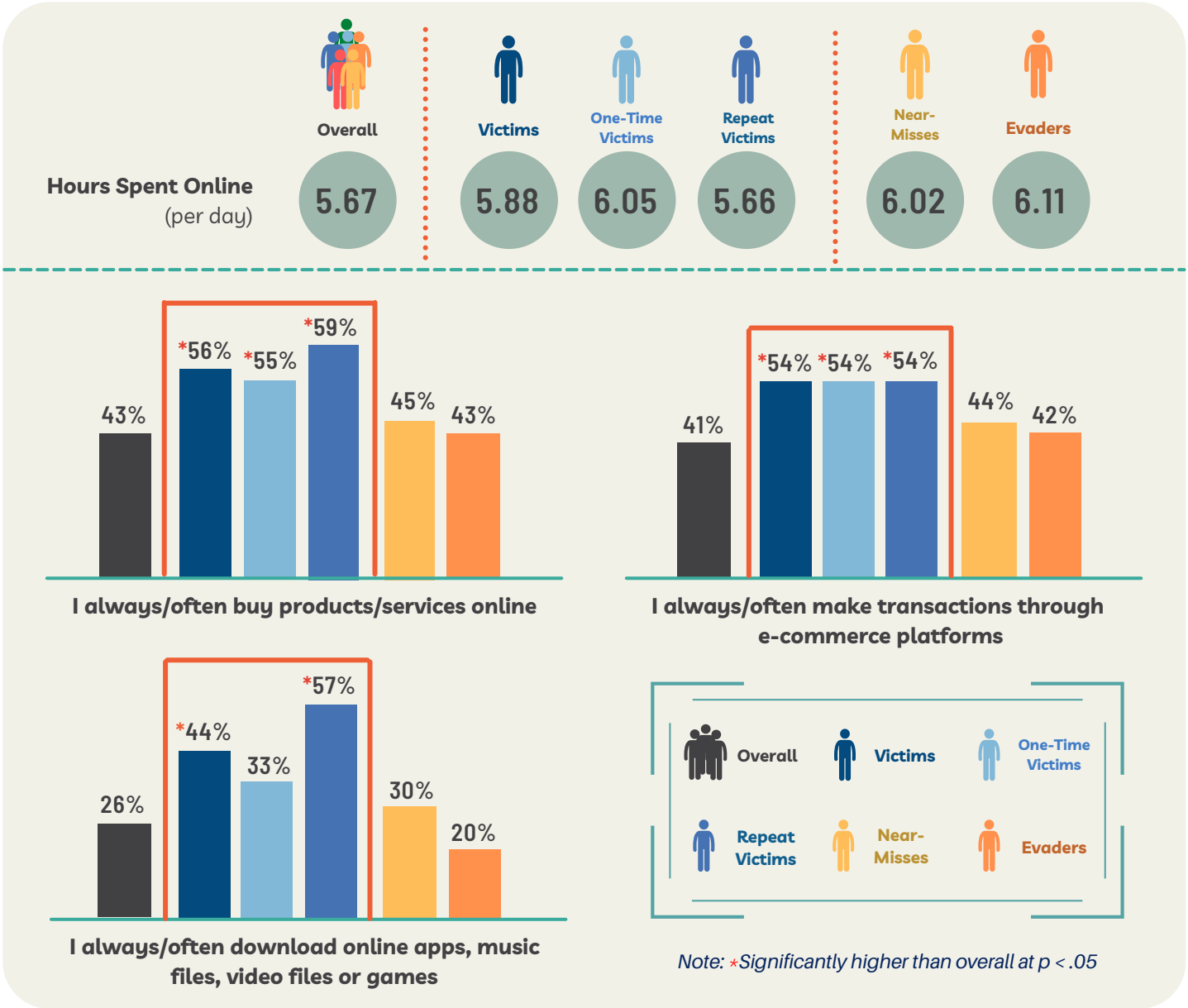


Figure 12: Online usage and activities compared across groups

Online Hygiene Practices

Furthermore, victims tend to display poorer online hygiene practices compared to near-misses and evaders. To illustrate, more victims reported frequently clicking on pop-up advertisements on websites or applications, opening emails from unknown senders, clicking on links without knowing what it might lead to, and signing up for free limited-time trial offers. These risky behaviours may have resulted in victims' increased susceptibility to scams.

Knowledge on Good and Safe Cyber Practices

Finally, a greater proportion of victims endorsed unsecure practices, increasing their vulnerability to scams. The NPSS included a quiz on cyber-hygiene to assess respondents' knowledge of what are good and safe online practices. Almost half of the victims wrongly believed that it is safe to click on any links that requested for verification of personal details. A significant 37% of victims were unaware that it is unsafe to share One-Time Passwords (OTPs) and endorsed this behaviour as common practice. More examples of victims' responses to the cyber-hygiene quiz included in the survey are depicted in Figure 13.

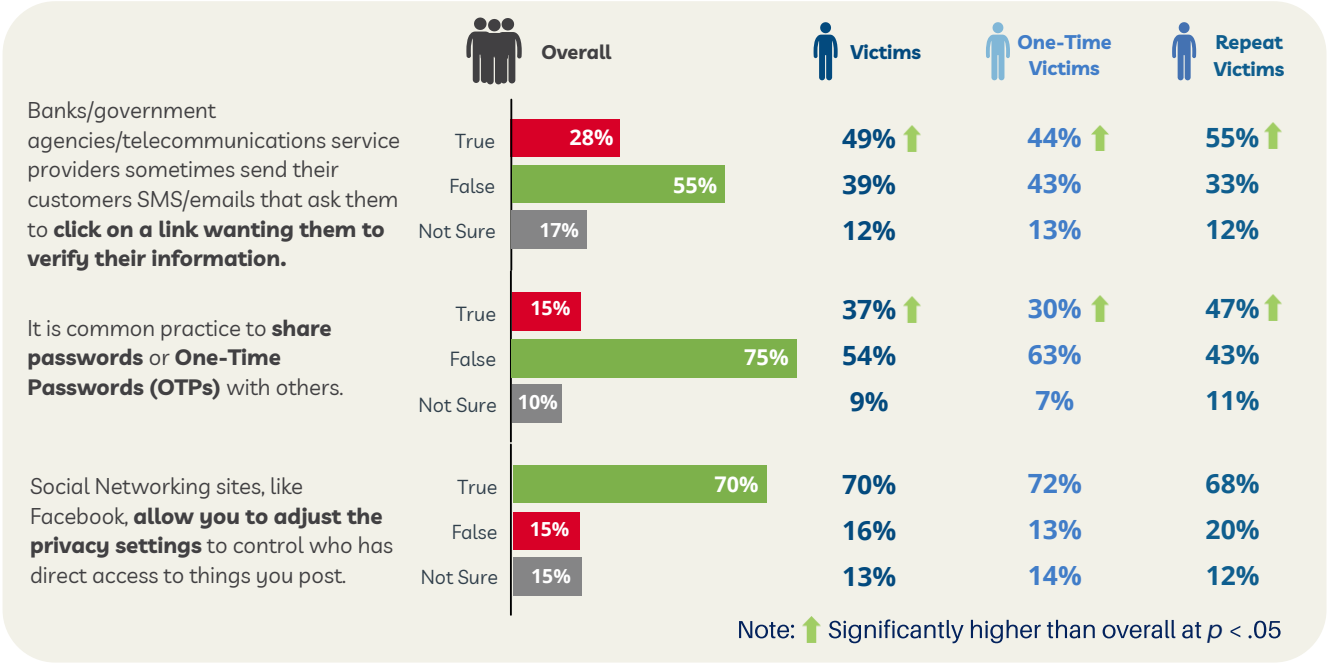


Figure 13: Victims' responses on some of the items of the cyber hygiene quiz

Why Did They Fall Prey?: Psychological Insights

Individual Traits and Attitudes

In the survey, the individual traits and attitudes of respondents were studied using validated psychometric scales. The findings suggest that compared to non-victims, victims tend to display strong traits of impulsivity and compliance. For instance, a significantly greater proportion of victims agreed to statements such as '*I need to act immediately when I see a bargain*' (i.e., impulsivity) and '*I find it hard to say no to people I like*' (i.e., compliance). Victims are also more self-conscious, easily influenced by others and tend to be complacent, believing that they are immune to scam victimisation or will get their losses back if they were to be scammed.

What was more intriguing was that victims were found to endorse greater cultural beliefs related to *kiasism* (i.e., attitude of being overly afraid or timid) and *kiasuism* (i.e., a grasping attitude arising from a fear of missing out on something) than non-victims. Such attitudes may increase, their vulnerability to scams as they are more likely to be enticed by a good deal or to comply with an authority figure or romantic partner, which are some of the scam tactics discussed earlier. Figure 14 illustrates these risky traits and attitudes.

Figure 14: Risky traits and attitudes of scam victims

Stress and Life Circumstances

Additionally, it was also found that compared to other groups, the victims, especially repeat victims, experienced higher levels of stress which may have put them in a more vulnerable emotional state, and hence at a greater risk of being susceptible to scams. As compared to the overall sample, a significantly larger proportion of victims reported that they had experienced elevated levels of stress as a result of stressful life events such as **negative changes in financial status (45%) as well as concerns about being lonely (31%).** Figure 15 illustrates the various other life events that had caused respondents to experience more stress.

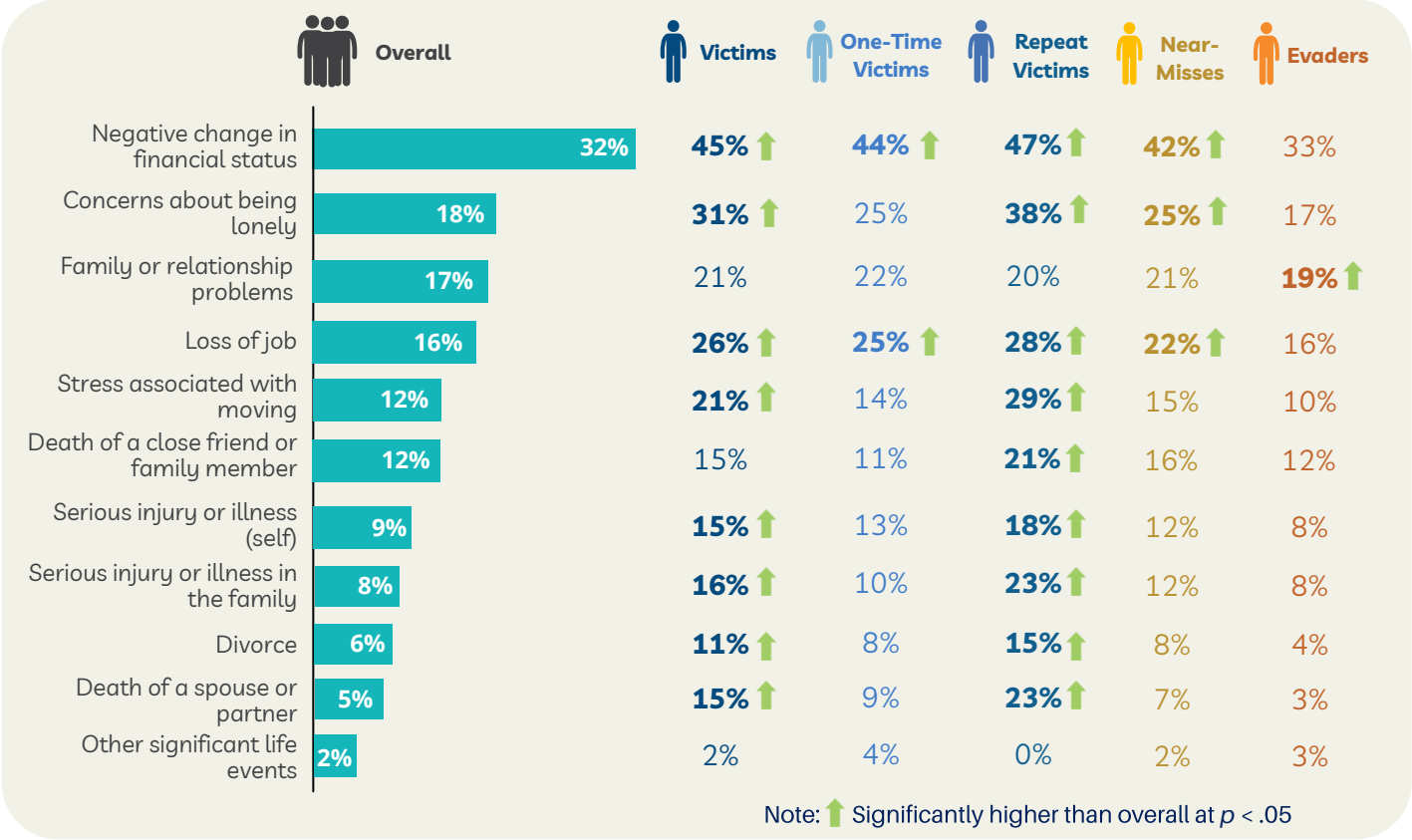


Figure 15: Various life events that reportedly increased stress levels experienced by respondents

Research has shown that the exposure to negative lifestyle changes and the occurrence of stressful life events are associated with an increased susceptibility to scam victimisation (Consumer Fraud Research Group, 2006; Ross & Smith, 2011; Shadel et al., 2014; Titus & Grover, 2001). As a result of life stressors such as social isolation and financial insecurity, individuals may experience an added strain that may place them at greater vulnerability to scam victimhood (DeLiema et al., 2019).

These changes in life circumstances can lead to the experience of higher levels of stress as individuals experience reduced stability and increased uncertainty in their current lives. It was found that, under high stress, individuals made decisions that tended to be less optimal due to a **reduced availability of cognitive resources needed to make decisions in a deliberate, considered and effortful manner** (Starcke & Brand, 2016; Wood et al., 2016). Furthermore, individuals under the effect of high stress were found to make poorer decisions overall as they tended to be **more enticed by the prospect of gaining rewards**, and were **more willing to engage in risk-taking behaviours** (Norris et al., 2019; Starcke & Brand, 2016; Titus & Grover, 2001).

Collectively, the effect of stress and life circumstances could have exposed victims to added risks for scam victimisation as victims made poorer quality decision under stress, and could have been in a more emotionally vulnerable state due to their experience of adverse life events and circumstances.

Scammers' Tactics

Online scams are constantly evolving and there are many reasons as to why the victims fell prey to scams. One reason is due to scammers' tactics becoming increasingly sophisticated in the dynamic digital world.

When examining the reasons why these victims fell prey to scams, the survey found that victims had indeed fallen into the traps of scammers' tactics, and the top reasons as to why they fell prey to scams include perceiving 1) a great bargain (27%), 2) the scammers as sincere, credible and convincing (23%), and 3) receiving a unique offer (22%) (Figure 16).

Other less cited reasons include **feeling understood** (20%), **getting something they were entitled to** (20%), and **following through with an agreement** (18%).

Figure 16: Top reasons for falling prey to scams

Scammers are known for their use of various persuasive tactics (e.g., the use of authority, scarcity, social proof, fake verifications, sunk cost, etc.) to override the victims' rational thinking, convincing them to give away their money and personal details. For example, the techniques of persuasion identified from the reasons why victims fell prey to scams are the use of scarcity when victims are made to perceive a great deal, the use of liking when victims perceive the scammer to be someone sincere or feel understood, or the use of consistency when victims wish to follow through with an agreement. Having a better understanding of these reasons and the persuasive tactics deployed by scammers could contribute to the formulation of new and improved anti-scam efforts.

Perceived Responsibility towards Scam Prevention

Finally, the perceived responsibility in keeping safe from scams may also play into an individual's vulnerability to scams as their perception may affect how they think about scams. Although 86% of victims showed **high awareness of anti-scam public campaigns**, they **continued to engage in risky online behaviour**. From the NPSS, it was found that a larger proportion of victims placed **greater emphasis on the Singapore Government's responsibility** in keeping Singaporeans safe from scams, and did not think that individual responsibility was a key factor for scam prevention. This perceived responsibility may have increased victims' scam vulnerability as they **downplayed the significance of individual efforts** in preventing scam victimisation. Ultimately, the best defence against scams is an informed and alert public.

Aftermath of a Scam

Monetary Losses

Scams are becoming a great concern in Singapore due to the significant losses and impact made on scam victims. Approximately three in four respondents reported being **negatively impacted** by their scam experience, with 13% of scam victims indicating that they were financially impacted. Based on comparison with available reports, Singapore has a higher median loss of SGD 713 as compared to the median loss of SGD 267 and SGD 430 in England and Wales, and the United States respectively (Office for National Statistics, 2020; Federal Trade Commission, 2020). In comparison to Australia, Singapore also has a significantly higher mean loss of SGD 37,227 than the mean loss of SGD 7,070 in Australia (ACCC, 2020) (Figure 17).

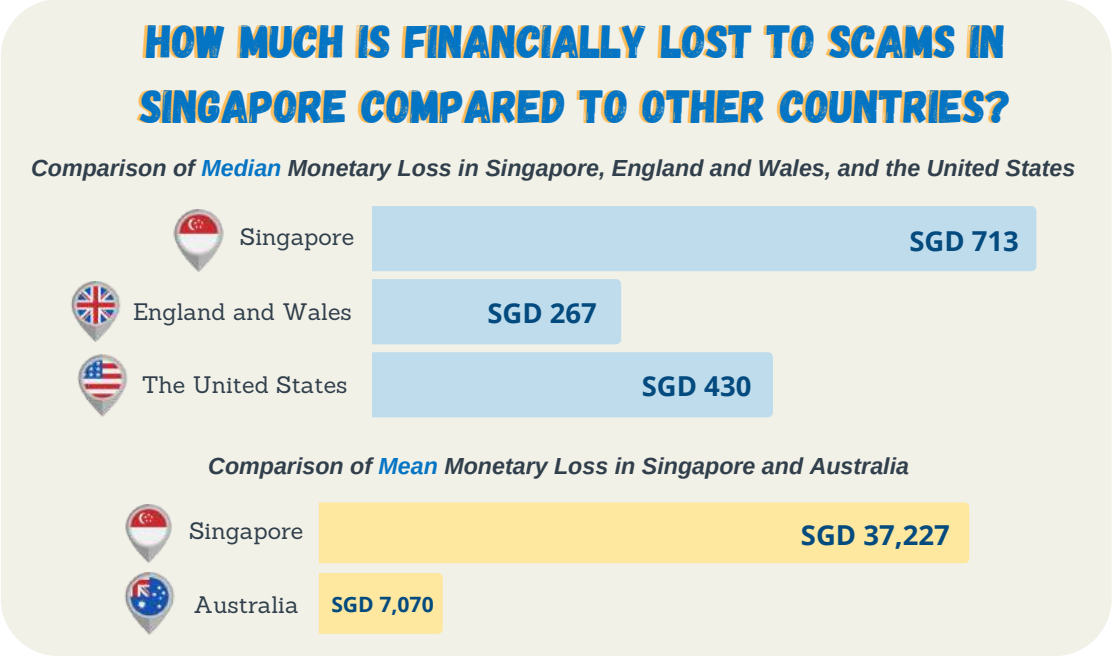


Figure 17: Financial losses compared across Singapore, the United States, England and Wales, and Australia

The top 10 most commonly used methods of payment as identified by the survey are (Figure 18):

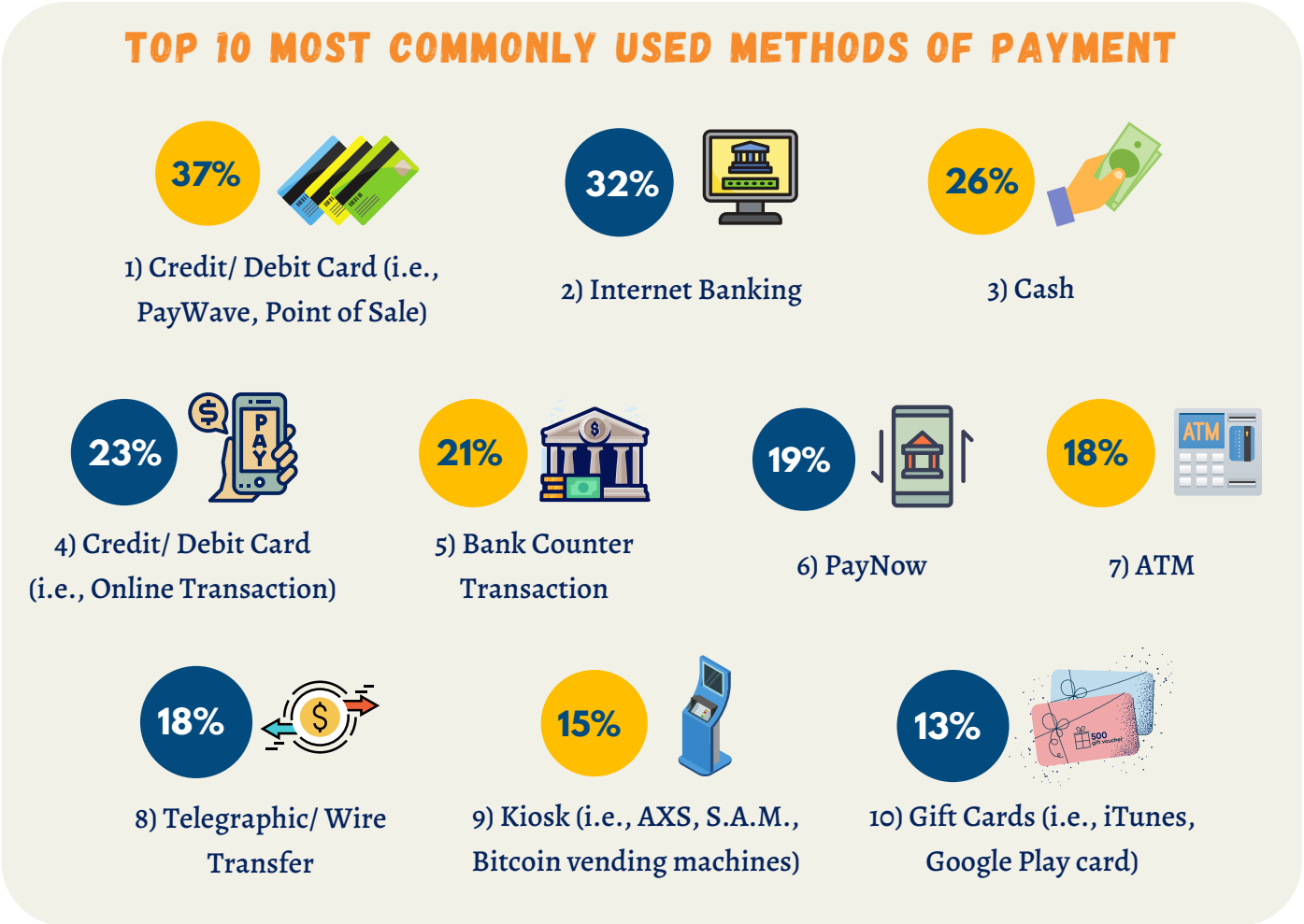


Figure 18: Top 10 most commonly used methods of payment

Emotional and Psychological Impact

In addition to experiencing a financial impact, a detrimental emotional and psychological impact was commonly reported as well. A quarter of scam victims (24%) who responded to the survey reported feeling sad, disappointed, or depressed after falling prey to a scam. On the flip side of the coin, 5% of respondents indicated that they became wiser and more cautious of scams after becoming a victim of scam (Figure 19).

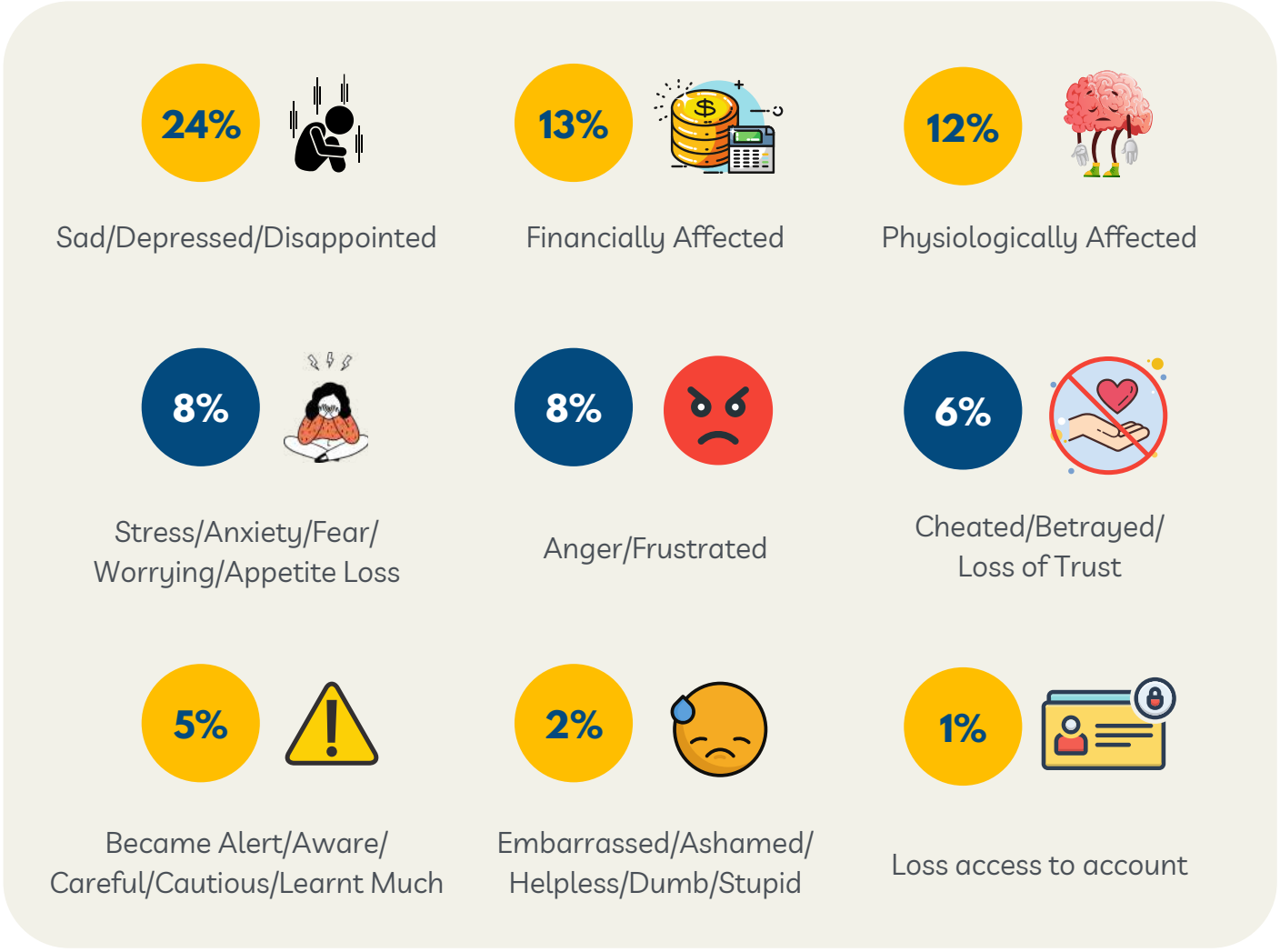


Figure 19: Various impacts of scams reported by victims

Although many perceive scams as a financial and "victimless" crime, the felt impact of scam victimisation can affect individuals in more serious ways than we imagine. Scams are not just about financial losses incurred. In fact, some scam victims may even experience significant emotional distress following the scam victimisation and some were at risk of developing post-traumatic stress. Victims' verbatim descriptions of how they felt following a scam experience can be found in Figure 20.

Figure 20: Victims' verbatim descriptions of the felt impact of scam victimisation

This survey also found that many victims continue to fall prey even after being a victim of scam once (i.e., repeat victims). There are two possible explanations pertaining to this finding. Firstly, repeat victims reportedly have a higher risk-taking outlook on life, possibly inhibiting them from being more vigilant and cautious even after being scammed once. Secondly, although repeat victims responded significantly higher to knowing someone that had previously fallen victim to a scam (72%), it is difficult to learn from others who have been scammed before as scam types and the scam landscape are constantly evolving.

Help-Seeking Behaviours

Despite experiencing the detrimental impact of being scammed, it was also found that only 50% of victims would seek informational advice or emotional support from their family and peers. 46% of victims chose not to seek help from family or friends due to reasons such as self-blame and feeling too embarrassed or ashamed to tell their loved ones about their scam experience. This highlights the significance of ensuring that support is provided to scam victims.

Reporting Behaviours

Further analysis of victims' reporting behaviours revealed that only 38% of victims made a police report immediately following the scam incident. On the contrary, seven in 10 victims informed organisations (e.g., banks, e-commerce sites, etc.) and individuals (e.g., family and friends) of the scam incident, intending to raise awareness and warn others about the scam (27%). Besides this, 15% of those who reported the scam to others (i.e., organisations and individuals) did so because they believed that banks or others could help resolve their problem. Similarly, the key reasons for reporting the scam incident to the police included wanting to get their money back by catching the scammers (14%).

Presently, what is more concerning is the group of victims who chose not to report the scam incident to the police or inform other authority figures such as banks or e-commerce platforms. As such, the NPSS also asked victims about their reasons for not reporting the scam incident. In terms of making a police report, it was found that more than half of victims (53%) perceived it to be a hassle, while 27% of them felt afraid to involve the police. In addition, more than 40% of victims engaged in self-blame and felt ashamed to report the incident to the police or other authorities. Another key reason for not informing other authorities is due to an unfamiliarity with the process of reporting (40%).

In addition to analysing the demographic, behavioural and psychological profile of scam victims, the following chapter looks into the profile of non-victims (i.e., near-misses and evaders) to better understand the types of behaviours and mindsets that serve as protective factors towards scam victimisation.

6

HOW TO AVOID SCAMS

Near-Misses: The Group who Nearly Fell Prey to Scams

Near-misses in the survey refer to individuals who, like victims, have engaged or interacted with scammers. However, they did not fall prey to a scam. According to the findings of the NPSS, 11% of the respondents reported almost becoming a victim of a scam.

To understand who was more likely to fall under the near-misses category, the survey identified factors that formed the near-miss profile. The demographic variables of the near-miss profile are as follows (Figure 21):

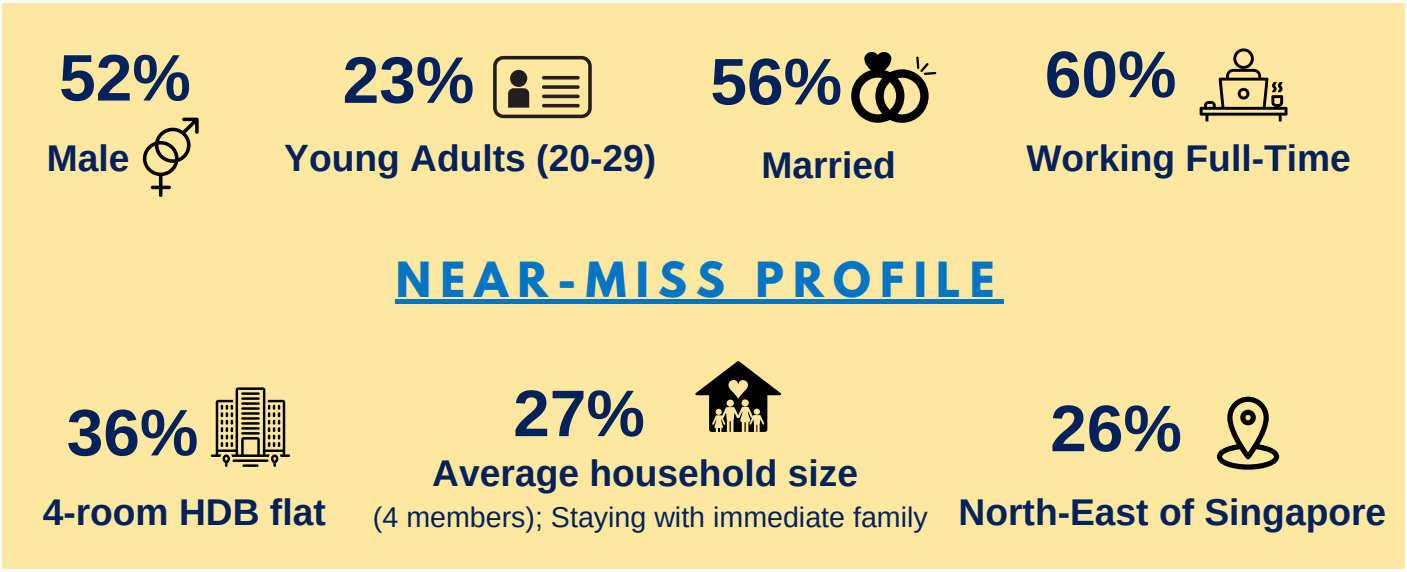
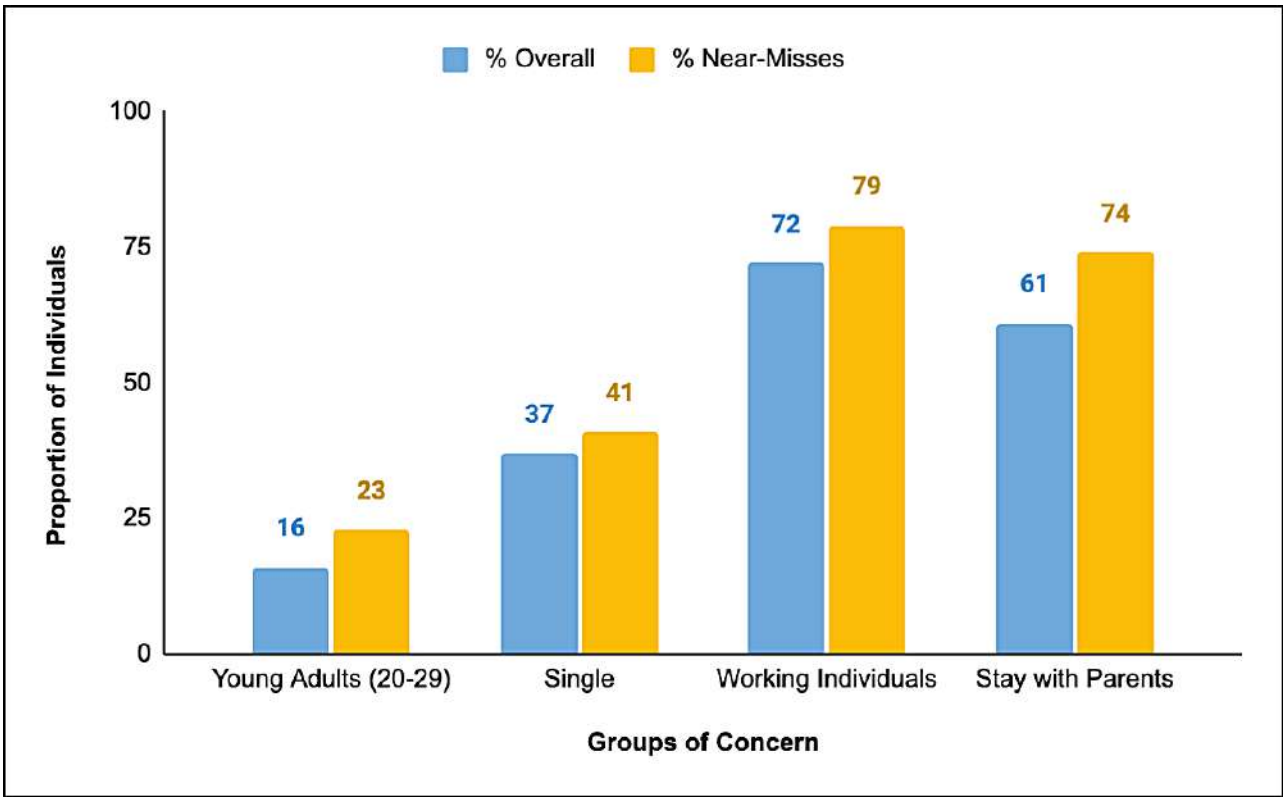


Figure 21: Demographic profile of near-misses

To identify at-risk groups of becoming near-misses, further analysis was also conducted to compare the sample of near-misses with the overall sample population to check for groups that were over-represented in this category of respondents. It was found that young adults between the age of 20 to 29, individuals who were single, working individuals, and those who lived with their parents were significantly over-represented in the near-misses population as compared to the overall sample of respondents (Figure 22).



Note: The difference between % Overall and % Near-Misses are significant at $p < .05$.

Figure 22: Groups of concern among near-misses

This suggests that **young adults** and **working individuals** are not only more prone to becoming a victim of scam, but also at risk of nearly falling prey to scams.

What Did They Do?: Behavioural Insights

Although near-misses spent more time online, they did not often engage in as many online activities that increased their risk of encountering scams as compared to victims. In other words, in comparison to victims, near-misses less frequently bought products or services online, made transactions through e-commerce platforms, or downloaded online applications or files (Figure 12).

With regard to cyber-hygiene practices, near-misses displayed relatively healthier online practices than victims. For instance, while 30% of victims reported that they would often click on pop-up advertisements on websites or applications, only 15% of near-misses reported doing the same. Similarly near-misses were approximately half as likely as victims to open emails from unknown sources, click on links without being certain of what it led to, or sign up for free limited-time trial offers, thus decreasing their susceptibility to scam victimisation (Figure 23).

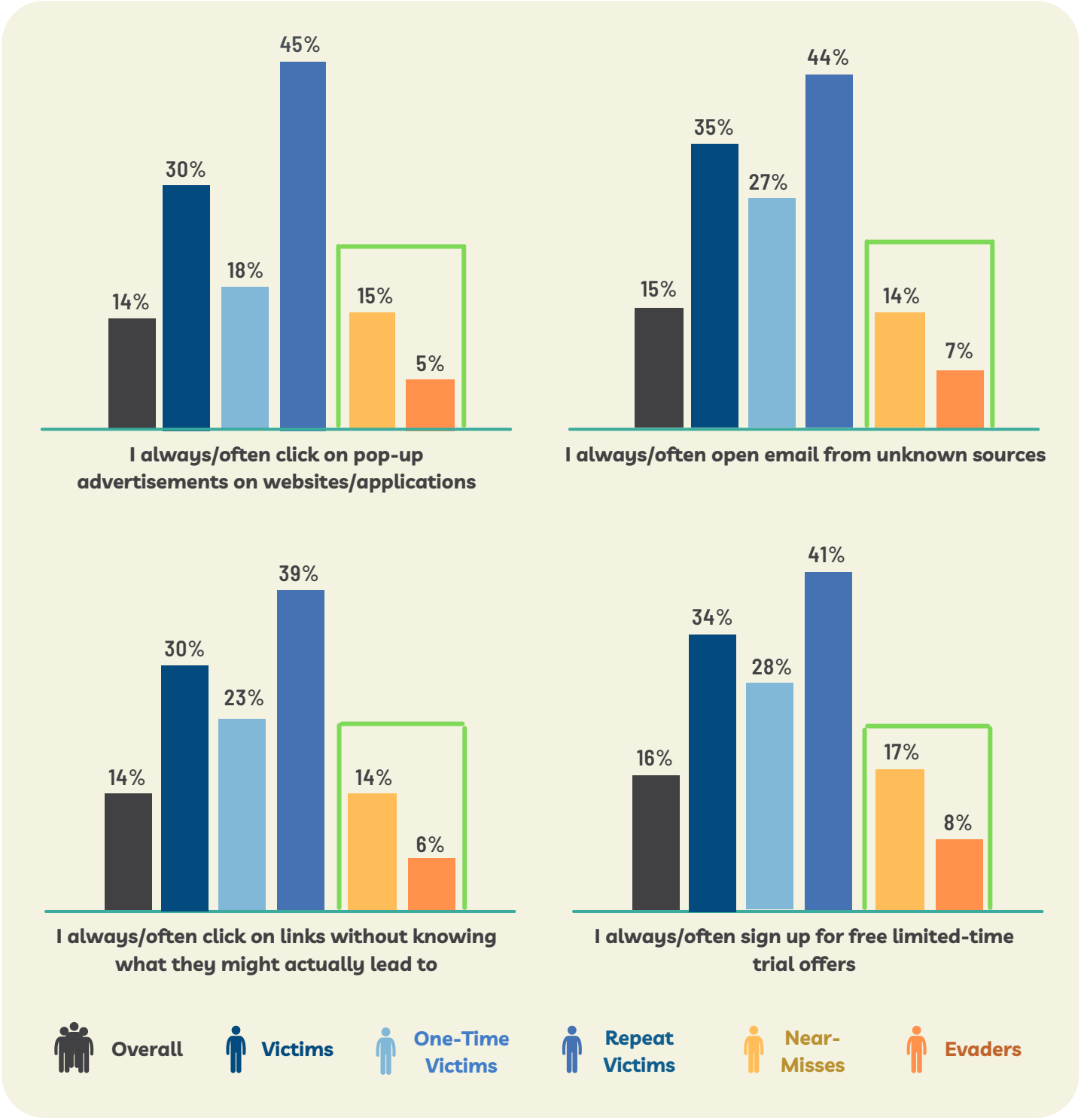


Figure 23: Online hygiene practices compared across groups

Finally, a significant proportion of near-misses behaved similarly to victims as they endorsed the practice of some unsecure cyber practices such as clicking on a link from banks or government agencies requiring them to verify their information. Despite their endorsements of a few unsecure cyber practices, near-misses still showed relatively **more awareness of good and safe cyber practices than victims**, which could have possibly contributed to the prevention of scam victimisation.

Why Did They Engage with Scammers but Were Not Victimised?: Psychological Insights

State of Mind

Near-misses shared **common reasons with victims** as to why they engaged with the scammer. These common reasons include 1) perceiving a good bargain (32%), 2) believing the scammers were sincere, credible and convincing (26%), and 3) receiving deals that were unique and rare (21%) (Figure 24).

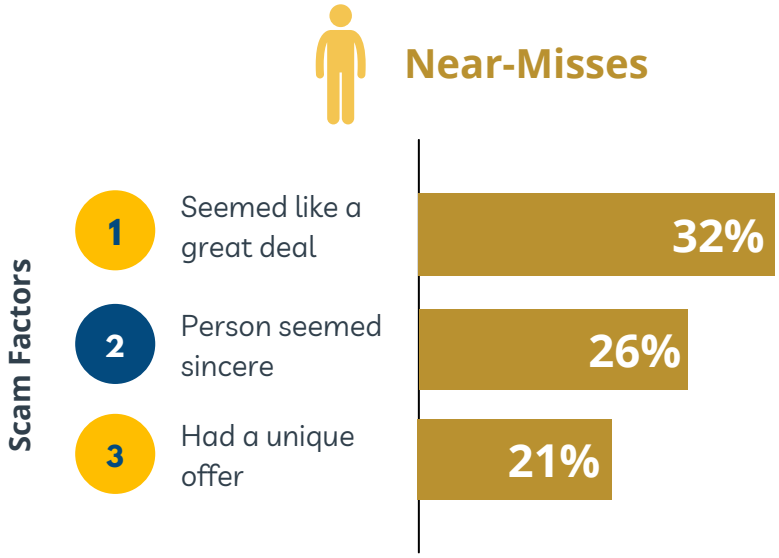


Figure 24: Top reasons for falling prey to scams

Individual Traits and Attitudes

Based on the psychometric scales, near-misses tended to display moderate traits of impulsivity and compliance. However, unlike victims, they did not display characteristics of low self-esteem or complacency, nor did they endorse the attributes of *fear of losing out to others*. This potentially lowered their likelihood of falling prey to scams although their moderate traits of impulsivity and compliance might have led them to engage with scammers.

Apart from risk factors, protective factors of scam vulnerability were also examined. What significantly differentiated near-misses from victims was that near-misses showed signs of vigilance and would practice caution before acceding to scammers' requests. They would become sceptical and attempt to spot the various warning signs of scams. For example, near-misses were able to identify that some information of the offer did not make sense and that the details of the scam were suspicious. Near-misses also had better knowledge of various scam tactics, thus preventing them from becoming a victim of scams.

Guardianship and Social Support

Interestingly, it was also found that guardianship plays a crucial role in scam prevention. Scam susceptibility has been seen to be negatively associated with social support (James et al., 2014), indicating lower risk of victimisation with higher levels of social support. Victims of cybercrime are less likely to seek out social support if they have high levels of perceived control and low levels of self-blame following their victimisation experience (De Kimpe et al., 2020).

As scam victims are able to draw on instrumental support (information, advice, financial aid, etc.) and emotional support from their networks, they may be able to better cope with their scam experiences. As such, the presence (or lack thereof) of someone in one's social network to rely on for help and support in times of need is an important factor for intervention and remediation as well.

In line with the understanding that guardianship via social support is implicated in scam victimisation, near-misses also reported that apart from being equipped to identify signs of scams, advice from family and friends contributed to the prevention of them giving in to scammers. In contrast, victims reported higher levels of stress and lower levels of social support.

Evaders: The Group who Evaded Scams

Finally, evaders are respondents who were approached by scammer(s) over the past year but did not engage with the scammer(s) and successfully evaded the consequences of a scam. Based on the survey sample, 45% of respondents had encountered scam(s) in the past year but had not engaged in the scam. Majority of them were (Figure 25):

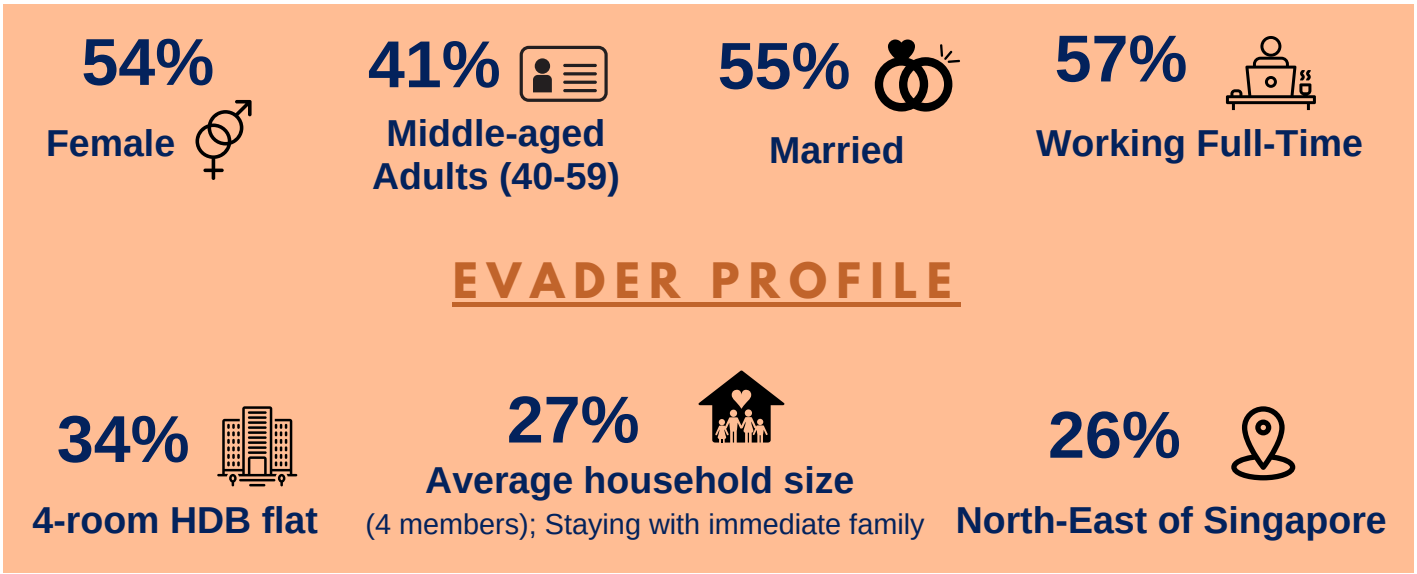
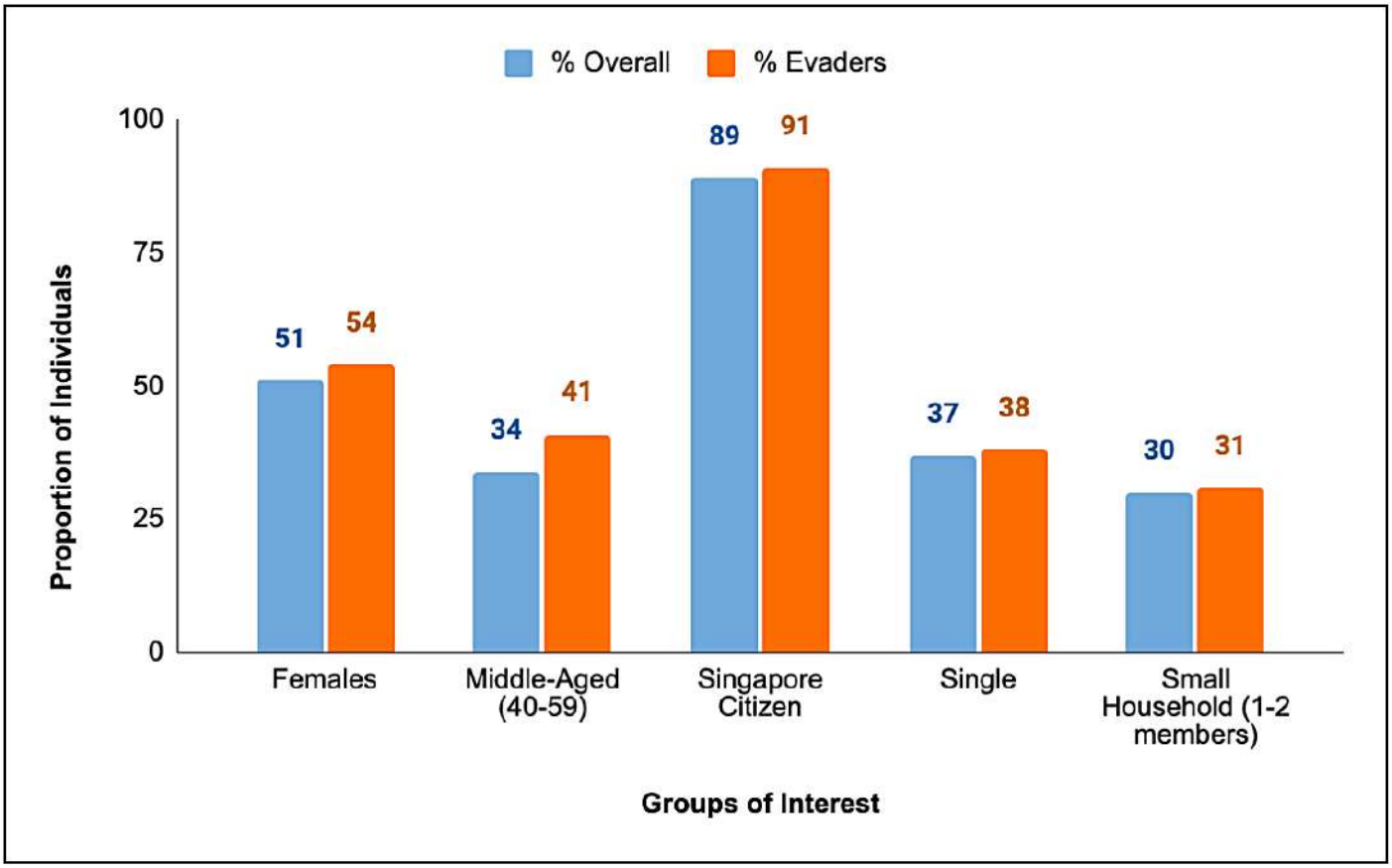


Figure 25: Demographic profile of evaders

In a similar vein, groups of interest that were over-represented in the sample of evaders in this survey were also identified. Here, the groups of interest highlighted are the groups of respondents who were more successful in evading scams compared to others (Figure 26).



Note: The difference between % Overall and % Evaders are significant at $p < .05$.

Figure 26: Groups of interest among evaders

What Did They Do To Evade Scams?: Behavioural Insights

Although evaders spent the most amount of time online (6.11 hours per day), they did not engage in online activities (i.e., buying products/services online, making transactions through e-commerce platforms, downloading files online) that increased their amount of exposure to scam encounters, thus minimising the likelihood of scam victimisation (Figure 12).

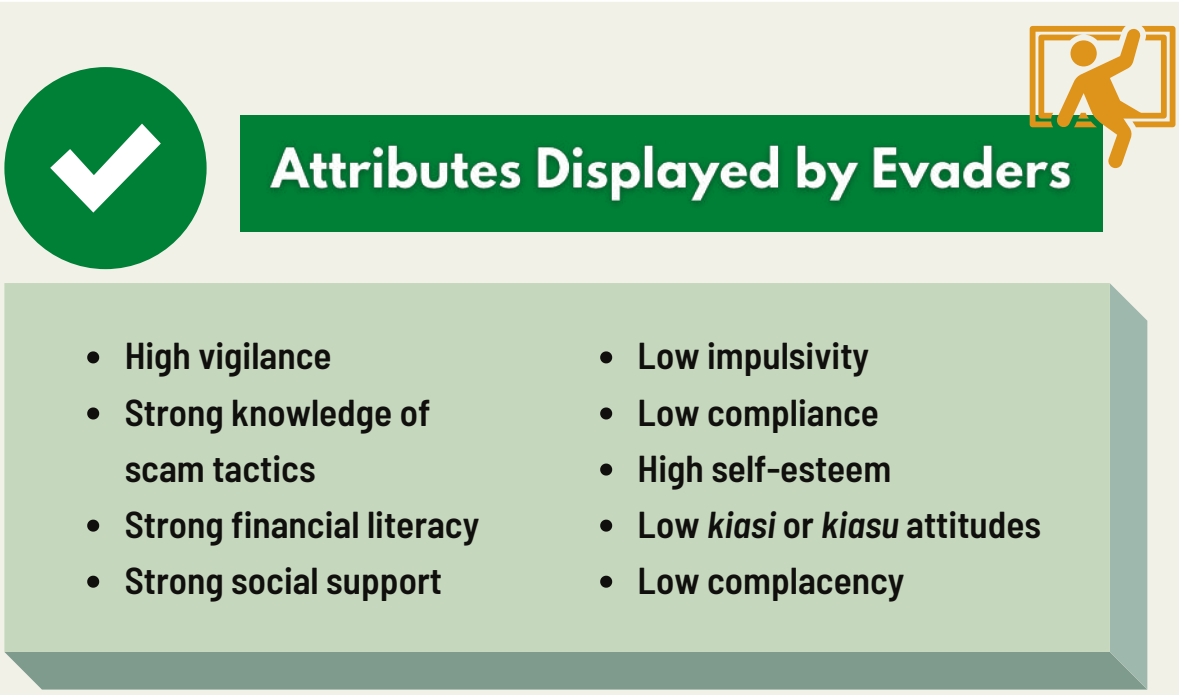
Evaders also tended to avoid risky behaviours such as clicking on pop-up advertisements (5%), opening emails from unknown sources (7%), clicking on links without knowing what they might actually lead to (6%), or signing up for free limited-time trial offers (8%) (Figure 23). Additionally, evaders were less likely to endorse unsecure cyber practices and displayed significantly greater awareness of protective online practices. Thus, contrary to victims' behaviours, evaders' online activities, good online hygiene practices and strong knowledge of good and safe cyber practices likely contributed to their successful evasion of scam victimisation.

Why Were They Less Vulnerable to Scam Victimisation?: Psychological Insights

Individual Traits and Attitudes

For evaders, they reported not getting involved with the scammers at all as **they were well-equipped with knowledge to identify scammers' tactics**. For instance, almost 70% of evaders claimed that they did not entertain the scam approach as they immediately knew it was a scam or would usually ignore calls, texts, or emails from unknown senders, indicating high vigilance.

Evaders displayed the least of the risky traits and attitudes compared to other groups. From the survey, evaders displayed the **highest level of self-esteem** and the **lowest level of impulsivity, compliance, *kiasi* or *kiasu* attitudes, and complacency**. Instead, they displayed the highest level of protective attitudes and behaviours such as **vigilance, knowledge of scam tactics, financial literacy, and social support**.



More specifically, evaders displayed higher levels of vigilance and were equipped with substantial knowledge of scams and scam tactics. From the survey, most evaders were '*always careful to check out people/companies if I haven't bought from them before*' (i.e., vigilance) and were '*aware of the various ways scammers use to scam*' (i.e., knowledge of scam tactics.).

Moreover, evaders showed awareness that they were not immune to becoming a victim of scams. They had strong social support and will readily verify with others if they are unsure whether they had encountered a scam. They also displayed strong financial literacy as well as good cyber hygiene practices.

Finally, while victims placed more emphasis on the Singapore Government's role in scam prevention, a large proportion of evaders perceive scam prevention to be largely the responsibility of the individual to keep themselves safe from becoming a victim of scams.

What Can We Learn from Non-Victims?

There is much we can glean from **those who have avoided the consequences of scams**. We learned that **near-misses and evaders were prevented from falling victim to scams as a result of**:

Being Healthy Sceptics

- Being alert to the **possible risks** of encountering scams in everyday life

Having Good Social Support

- E.g., from those who care and look out for them by **warning them about scams**
- Advice from family, friends, and colleagues played an **important role** in preventing this group from giving in to scammers' requests

Personal Alertness and Caution

- They had **second thoughts**
- They decided to **investigate** further
- They **remembered** how others had been scammed
- They were **alert to anti-scam messages**

7

A MULTI-PRONGED APPROACH TO SCAM PREVENTION

To effectively fight scams, we will require a collective national effort that enlists the efforts of individuals, the community, enterprises and the Government.

Policy Level Efforts

The Inter-Ministry Committee of Scams (IMCS), led by Minister of State for Home Affairs and Ministry of Sustainability and the Environment, Mr Desmond Tan, was set up to arrest the rise in scams. The IMCS leverages on expert knowledge and resources from different government agencies such as the Ministry of Home Affairs (MHA), the Ministry of Communications and Information (MCI), the Ministry of Trade and Industry (MTI), and the Monetary Authority of Singapore (MAS) to coordinate the Government's anti-scam efforts.

Since the set-up, IMCS has been focusing on three areas:

1. Partnering stakeholders to combat scams
2. Strengthening enforcement
3. Public education

For example, through partnership with banks, the Association of Banks Singapore (ABS) and its members have worked with the Singapore Police Force (SPF) and the MAS to identify scammers and money mules. A scam awareness quiz was also launched this year to educate the public on scams and encourage good cyber hygiene habits. The SPF and ABS are working together to explore ways of enhancing the process of one-time pin verification and training of frontline bank staff to detect and intercept potential scams.

A MULTI-PRONGED APPROACH TO SCAM PREVENTION

Aside from banks, the IMCS has also leveraged on their partnerships with digital and e-commerce platforms (e.g., Carousell, Lazada, and Shopee) with the aim of preventing scams through improving seller verifications and increasing the use of more secure payment methods (e.g., escrow accounts). Additionally, the IMCS also partners closely with telcos to aid in their scam prevention efforts as they work closely to block spoof calls or scam websites used by international scammers.

Last year, the Infocomm Media Development Authority (IMDA) and telcos introduced the '+' prefix initiative for all overseas calls entering Singapore. This has helped to alert the public of potentially suspicious and spoofed calls from overseas scammers.

Additionally, the committee has tapped on technology and works with the community to prevent scams by encouraging Singaporeans to download the ScamShield application.

The ScamShield application, which was developed by the Government Technology Agency of Singapore (GovTech) and the National Crime Prevention Council (NCPC), was launched in November 2020 (Figure 27). Since its launch, ScamShield has proven effective in reducing the opportunities for scammers to reach out to victims as it is reportedly **blocking over 8,600 suspected scam numbers** and has **sieved out more than 1.4 million scam messages**.

Figure 27: ScamShield Phone Application (Sun, 2021)

IMCS INITIATIVES WITH THE VARIOUS PARTNERS

Banks

Identify scammers and money mules.

Singapore Police Force

Help scam victims recover their losses.

E-commerce Platforms

Improve seller verification and increasing use of more secure payment methods.

Community

Encourage Singaporeans to download the ScamShield application.

Operational and Law Enforcement Efforts

To improve detection and disruption of scams, the SPF adopts a multi-pronged approach to tackle the rise in scams, specifically through the strategies as follows (SPF, 2021):

- Strengthening domestic enforcement against scam perpetrators;
- Increasing collaboration with foreign legal enforcement agencies to disable or disrupt crime groups targeting Singapore;
- Working with various public and private stakeholders to tackle commercial crime;
- Continued efforts at educating the public on how they can protect themselves from falling prey to scams; and
- Constant innovation and use of technology to tackle scams.

For instance, the Anti-Scam Division (ASD) from SPF has also collaborated with over thirty financial institutions on Project FRONTIER (Funds Recovery Operations and Networks Team, Inspiring Effective Resolutions) to disrupt scammers' operations. This has vastly improved the efficiency to intercept a scam operation as once the police are notified of a possible scam activity, most bank accounts that are suspected to be involved in scammers' operations can now be quickly frozen within a day when it previously required 14 to 60 working days.

As many scams involve syndicates overseas, the ASD also works closely with foreign law enforcement agencies in crippling these syndicates. For example, in June 2021, through strong information-sharing and collaboration by ASD, six transnational syndicates perpetrating job scams, internet love scams and China official impersonation scams were busted by the Royal Malaysian Police, Hong Kong Police Force and Taiwan Police.

Public Prevention and Education Efforts

While all these measures contribute significantly to Singapore's fight against scams, the best defence Singapore could have against scams is for the public to practice caution and vigilance.

In partnership with the NCPC, MHA has focused on more significant outreach efforts towards public education on potential scam indicators. The latest anti-scam campaign, "*Spot the Signs. Stop the Crimes.*" aims to educate members of the public on how to spot the tell-tale signs of various scams through sharing of tactics used by scammers. With scammer tactics

constantly evolving, MHA and NCPC have also stepped up the efforts to educate the public on changing scam tactics. Some examples of initiatives to raise public awareness on the various scam types are shown below (Figure 28 & Figure 29).

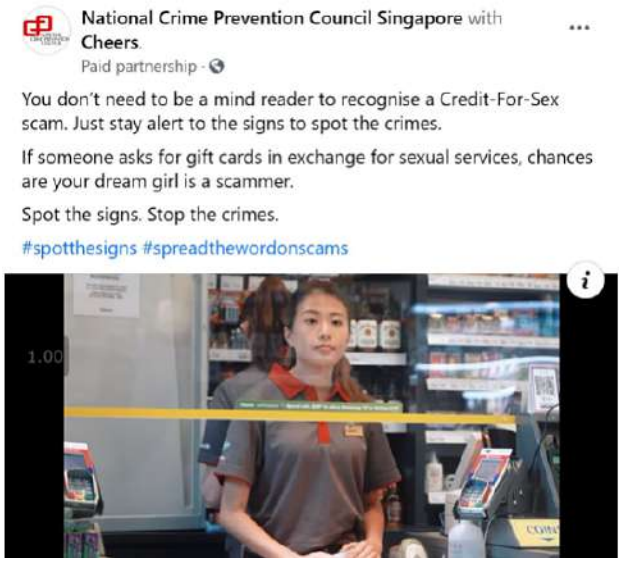


Figure 28: Social media video on credit-for-sex scam (adapted from the National Crime Prevention Council Singapore Facebook page, 2021b)

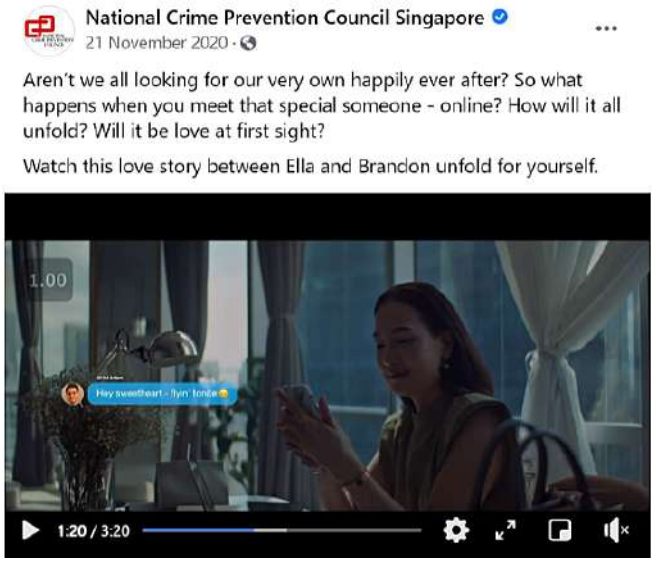


Figure 29: Social media video on internet love scam (adapted from the National Crime Prevention Council Singapore Facebook page, 2020)

Together with NCPC, the SPF has also been adopting innovative strategies to educate the public on how they can protect themselves from falling prey to scams such as, through the use of scam-related memes on social media (Figure 30) and the "safe-tea" campaign with promotion for bubble tea beverages that came with scam advisory printed on the cup cover (Figure 31).

Figure 30: Meme on e-commerce scam (from National Crime Prevention Council Singapore Facebook page, 2021c)

Figure 31: The Safe-tea campaign in early 2021 (from National Crime Prevention Council Singapore Facebook page, 2021a)

Community Efforts

The community, which includes members of the public as well as business operators such as e-commerce platforms, banks and telecommunication companies, all have important roles to play in tackling the rise in scams in Singapore. Business operators could deter scams via anti-scam measures on their platforms to keep their customers safe from scams.

From the survey, the findings revealed that social support and family/peer advice played an important role in preventing the near-misses from becoming victimised. Family members and friends can play their part in preventing their loved ones from falling prey to scams by being aware of these threats and cautioning their loved ones about them. The SPF has worked with business operators in putting measures in place to keep their consumers safe. In addition, business operators are also actively involved in promoting anti-scam public education materials. For instance, the 'Mata-Bytes' initiative by Punggol Neighbourhood Police Centre (NPC), an interview session conducted live on Facebook, invited the Senior Vice President of e-commerce platform Lazada to share tips on safe shopping.

The NCPC has also put in place various scam prevention initiatives to encourage the community to keep their guard up against scams. An example would be the aforementioned ScamShield application that was created in collaboration with GovTech to reduce the likelihood of the community encountering scams and falling prey as a result.

> We hope that with this ScamShield app, it will provide the public with some **form of protection** and shield them **from these "invisible enemies"**. While we have this app, we urge the public to continue to **stay vigilant** and not let their guard down."
>
> **Mr Gerald Singham**
> **Chairman of NCPC**

Besides a strong social media presence with anti-scam social media campaigns, NCPC also created a channel on the online messaging application, Telegram, to warn the community about new scam types and urge the public to forward these anti-scam advisories and videos to their loved ones (Figure 32).

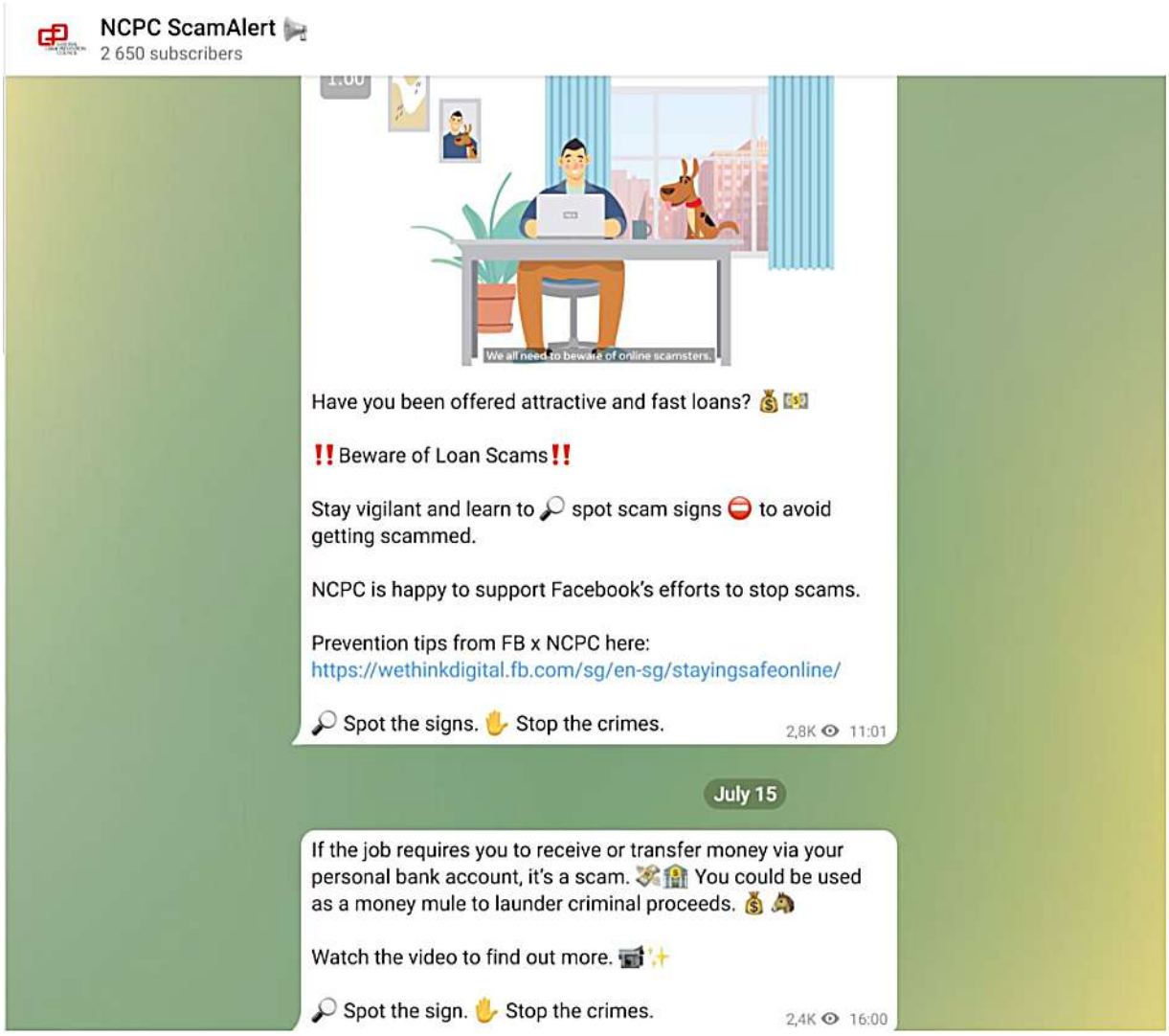


Figure 32: Screenshot of the National Crime Prevention Council (NCPC) ScamAlert Telegram Channel (from NCPC ScamAlert, 2021)

Individual Efforts

Finally, individuals also have an important role to play in protecting themselves and their loved ones from falling prey to scams. As reflected from the survey findings, those who had attributed a lower level of individual responsibility in safeguarding against scams were more likely to fall prey to scams instead.

Moreover, everyone can keep their loved ones safe by adopting a number of methods. Firstly, Singaporeans could ensure they remain updated on the latest scam trends and tips. To do so, one can subscribe to channels such as ScamAlert to receive notifications on the latest scam types and trends. By being informed through such channels, individuals can then help to spread the information to their loved ones.

Another way individuals can keep themselves and their loved ones safe from scams is to encourage conversations about scams. From the survey, many near-misses avoided falling prey to scams due to the advice received from their family and peers. Hence, these conversations can be focused on sharing tips to avoid becoming a victim of scam or can revolve around the topic of what type of scams they have encountered or how often they have previously encountered scams in order to increase awareness of the various scam types and tactics. By creating a space for individuals to openly speak about their scam encounters, it could serve as motivation for loved ones to verify any possible scam attempts with each other, minimising their risks of falling prey to a scam.

Linking back to the survey, Singaporeans can defend themselves against scams by remembering and practicing the 6S Anti-Scam Self-Protection Principles as listed below (Figure 33):

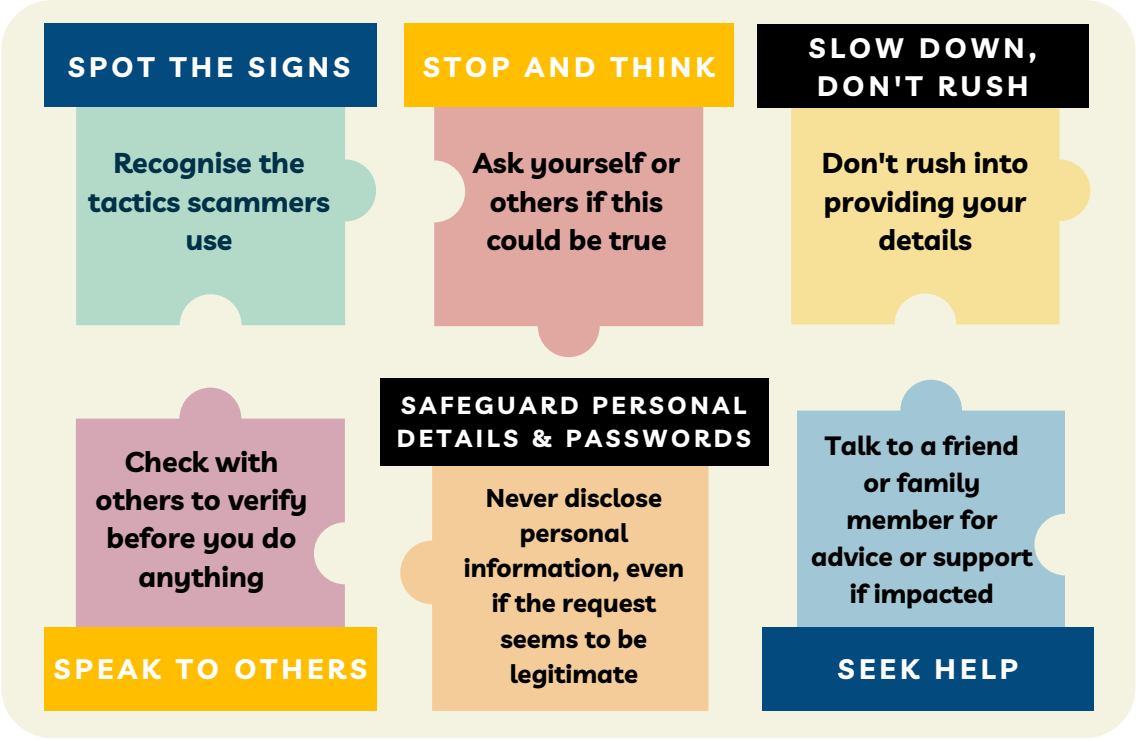


Figure 33: The 6S Anti-Scam Self-Protection Principles

Conclusion

The government will continue to lead the anti-scam efforts, but everyone plays a part in this fight against scams. Each partner in the industry and community can shed new insights about the scam situation from a unique angle and therefore, offer a unique solution to Singapore's scam situation. As highlighted in this book, individuals can also make a big difference by keeping themselves updated on latest scam trends, recognising signs of scams and watching out for their loved ones. This book therefore serves as a general guide for anyone to fight against scams.

References

ABC News. (2017, February 27). *Psychology of scams: The emotional traps to watch out for*. https://www.abc.net.au/news/2017-02-27/psychology-of-scams/8306060

Action Fraud (2020, July). *Fraud Crime Trends 2019-20*. https://data.actionfraud.police.uk/cms/wp-content/uploads/2020/07/Fraud-crime-trends.pdf

Almazora, L. (2021, February 8). *Frauds surged across Canada in 2020 amid pandemic*. Wealth Professional Canada. https://www.wealthprofessional.ca/news/industry-news/frauds-surged-across-canada-in-2020-amid-pandemic/337595.

Anderson, K. (2019, October). *Mass-market consumer fraud in the United States: A 2017 update*. Federal Trade Commission. https://www.ftc.gov/system/files/documents/reports/mass-market-consumer-fraud-united-states-2017-update/p105502massmarketconsumerfraud2017report.pdf

Arkes, H. R., & Blumer, C. (1985). The psychology of sunk cost. *Organizational Behavior and Human Decision Processes, 35*(1), 124-140. doi:10.1016/0749-5978(85)90049-4

Asokan, A. (2020, March 27). *MOH warns of scammers Impersonating its employees, COVID-19 contact Tracing teams*. Channel News Asia. https://www.channelnewsasia.com/singapore/moh-covid19-scam-automated-call-impersonating-health-officials-1325286.

Australian Bureau of Statistics (2016, April 20). *Personal fraud: 2014-15*. https://www.abs.gov.au/statistics/people/crime-and-justice/personal-fraud/latest-release

Australian Competition and Consumer Commission (2020, June). *Targeting scams 2019: A review of scam activity since 2009*. https://www.accc.gov.au/system/files/1657RPT_Targeting%20scams%202019_FA.pdf

Australian Competition and Consumer Commission (2021, June). *Targeting scams: Report of the ACCC on scams activity 2020*. https://www.accc.gov.au/system/files/Targeting%20scams%20-%20report%20of%20the%20ACCC%20on%20scams%20activity%202020%20v2.pdf

Baker, S. R., Bloom, N., Davis, S. J., & Terry, S. J. (2020). *Covid-induced economic uncertainty* [NBER Working Paper No. 26983]. National Bureau of Economic Research.

BlueVoyant. (2020). *Top 5 cybercrimes and prevention tips*. https://www.bluevoyant.com/blog/top-5-cybercrimes-and-prevention-tips/

Brignull, H. (n.d.). *Types of dark pattern*. https://www.darkpatterns.org/types-of-dark-pattern

Button, M., & Cross, C. (2017). *Cyber frauds, scams and their victims*. Routledge.

Button, M., Lewis, C., & Tapley, J. (2009). *Fraud typologies and the victims of fraud: Literature review.* National Fraud Authority. https://researchportal.port.ac.uk/portal/files/1926122/NFA_report3_16.12.09.pdf

Button, M., Lewis, C., & Tapley, J. (2012). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal, 27*(1), 36–54. https://doi.org/10.1057/sj.2012.11

Canadian Anti-Fraud Centre (2020, February 17). *Financial crime trend bulletin: The top 10*. Canadian Anti-Fraud Centre Bulletin. https://cacpc.ca/uploads/3/4/4/8/34487623/2020.02.17_-_top_10_frauds___prevention_tips.pdf

Canadian Anti-Fraud Centre (2021, February 01). *2020 top 10 frauds targeting Canadians*. Canadian Anti-Fraud Centre Bulletin. https://cacpc.ca/uploads/3/4/4/8/34487623/2021.02.01_cafc_top_10_in_2020.pdf

Chartered Professional Accountants of Canada (2021, February 22). *CPA Canada 2021 annual fraud study – backgrounder*. https://cpacanada.ca/fraud2021?_ga=2.194753444.801940007.1626319693-59432079.1612755653

Chan, M., Regalado, F., & Cheng, T. (2020, March 4). Coronavirus scams prey on the fearful in China, Japan and beyond. *Nikkei Asian Review*. https://asia.nikkei.com/Spotlight/Coronavirus/Coronavirus-scams-prey-on-the-fearful-in-China-Japan-and-beyond

Cialdini, R. B. (2001). The science of persuasion. *Scientific American, 284*(2), 76-81. https://doi.org/10.1038/scientificamerican0201-76

Cialdini, R. B. (2016). *Pre-suasion: A revolutionary way to influence and persuade*. Simon and Schuster.

Consumer Fraud Research Group. (2006, May 12). *Investor fraud study final report.* NASD Investor Education Foundation. Washington, DC. https://www.sec.gov/news/press/extra/seniors/nasdfraudstudy051206.pdf

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

Cyber Security Agency of Singapore. (2020, June 26). *Singapore cyber landscape 2019*. https://www.csa.gov.sg/en/News/Publications/singapore-cyber-landscape-2019

Cyber Security Agency of Singapore. (2021, July 08). *Singapore cyber landscape 2020*. https://www.csa.gov.sg/en/News/Publications/singapore-cyber-landscape-2020

De Kimpe, L., Ponnet, K., Walrave, M., Snaphaan, T., Pauwels, L., & Hardyns, W. (2020). Help, I need somebody: Examining the antecedents of social support seeking among cybercrime victims. *Computers in Human Behavior*, 108, 106310. https://doi.org/10.1016/j.chb.2020.106310

DeLiema, M., Fletcher, E., Kleffer, C., Mottola, G., Pessanha, R., & Trumpower, M. (2019). *Exposed to scams: What separates victims from non-victims?*.

European Consumer Centres Network. (2017). *Fraud in cross-border e-commerce*. https://ec.europa.eu/info/sites/default/files/online_fraud_2017.pdf

European Commission. (2020, January). *Survey on "scams and fraud experienced by consumers": Final report.* https://ec.europa.eu/info/sites/default/files/aid_development_cooperation_fundamental_rights/ensuring_aid_effectiveness/documents/survey_on_scams_and_fraud_experienced_by_consumers_-_final_report.pdf

Federal Trade Commission. (2021, February). *Consumer sentinel network data book 2020.* https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf

Fischer, P., Lea, S. E., & Evans, K. M. (2013). Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of scam compliance. *Journal of Applied Social Psychology, 43*(10), 2060-2072. https://doi.org/10.1111/jasp.12158

Fruhlinger, J. (2020, March 9). *Top cybersecurity facts, figures and statistics*. CSO Online. https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html

Gee, J., & Button, M. (2019). The financial cost of fraud 2019: The latest data around the world. Crowe UK. https://researchportal.port.ac.uk/portal/files/18625704/The_Financial_Cost_of_Fraud_2019.pdf

REFERENCES

Goldman, M. (1986). Compliance employing a combined foot-in-the-Door and door-in-the-Face procedure. *The Journal of Social Psychology, 126*(1), 111-116. https://doi.org/10.1080/00224545.1986.9713577

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

Haselton, M. G., Nettle, D., & Murray, D. R. (2015). The evolution of cognitive bias. *The Handbook of Evolutionary Psychology,* 1-20. https://doi.org/10.1002/9781119125563.evpsych241

Hong Kong Police Force. (2021). *Law and order situation in 2020.* https://www.police.gov.hk/ppp_en/01_about_us/cp_ye.html

Hong Kong Police Force Security Bureau. (2021, May). *Legislative council panel on security initiatives for preventing and combating deception cases* [LC Paper No. CB(2)1110/20-21(03)]. https://www.legco.gov.hk/yr20-21/english/panels/se/papers/se20210601cb2-1110-3-e.pdf

Interpol. (2020, August). *Cybercrime: COVID-19 impact.* https://www.interpol.int/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf

International Mass-Marketing Fraud Working Group (2010, June). Mass-marketing fraud: A threat assessment. https://www.fincen.gov/sites/default/files/shared/IMMFTAFinal.pdf

International Public Sector Fraud Forum. (2020, February). Guide to understanding the total impact of fraud. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/866608/2377_The_Impact_of_Fraud_AW__4_.pdf

Jakobsson, M. (2016). Understanding social engineering based scams. Springer.

James, B. D., Boyle, P. A., & Bennett, D. A. (2014). Correlates of susceptibility to scams in older adults without dementia. Journal of Elder Abuse & Neglect, 26(2), 107-122. https://doi.org/10.1080/08946566.2013.821809

Johnson, J. (2021). Worldwide digital population as of January 2021. Statista. https://www.statista.com/statistics/617136/digital-population-worldwide/

Kirwan, G. H., Fullwood, C., & Rooney, B. (2018). Risk factors for social networking site scam victimization among Malaysian students. Cyberpsychology, Behavior, and Social Networking, 21(2), 123-128. doi:10.1089/cyber.2016.0714

Lea, S. E., Fischer, P., & Evans, K. M. (2009). The psychology of scams: Provoking and committing errors of judgement.

Levi, M. (2008). Organized fraud and organizing frauds: Unpacking research on networks and organization. Criminology & Criminal Justice, 8(4), 389-419. https://doi.org/10.1177/1748895808096470

Levi, M. & Smith R. (2021). Fraud and its relationship to pandemics and economic crises: From Spanish Flu to COVID-19. (AIC Research Report 19). Australian Institute of Criminology. https://apo.org.au/sites/default/files/resource-files/2021-05/apo-nid312080.pdf

Lo, C. (2021, February 15). Over HK$8 billion from scam victims laundered through Hong Kong bank accounts in 2020: police sources. South China Morning Post. https://www.scmp.com/news/hong-kong/law-and-crime/article/3121789/over-hk8-billion-scam-victims-laundered-through-hong

Lo, C. (2020, March 02). Hong Kong police intercept more than US$384 million swindled from victims of internet and phone scams around the world. South China Morning Post. https://www.scmp.com/news/hong-kong/law-and-crime/article/3064633/hong-kong-police-intercept-more-us384-million-swindled

Ma, K. W. F.., & McKinnon, T. (2021). COVID-19 and cyber fraud: emerging threats during the pandemic. Journal of Financial Crime.

Mertens, G., Gerritsen, L., Salemink, E., & Engelhard, I. (2020). Fear of the coronavirus (COVID-19): Predictors in an online study conducted in March 2020. Journal of anxiety disorders, 74, 102258. https://doi.org/10.31234/osf.io/2p57j

Miranda, C. (2014, December 8). How do scammers in your community connect with you?. Federal Trade Commission. https://www.consumer.ftc.gov/blog/2014/12/how-do-scammers-your-community-connect-you

Morgan, J. (2014, May 13). A simple explanation of "The Internet Of Things". Forbes. https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/?sh=74eb556d1d09

National Crime Prevention Council Singapore. (2020, November 21). *Aren't we all looking for our very own happily ever after? So what happens when you meet that special someone...* [Video]. Facebook. https://www.facebook.com/ncpc.sg/videos/288218665884978/

National Crime Prevention Council Singapore. (2021). NCPC ScamAlert [Telegram page]. Telegram. https://t.me/s/ncpcscamalert?before=4/

National Crime Prevention Council Singapore. (2021a, February 23). *Flash this post at any 1 of the 4 participating outlets to enjoy 1 for 1 promotion on all drinks! [Photograph]*. Facebook. https://www.facebook.com/ncpc.sg/photos/a.146829248684077/4109828202384142/?type=3&theater

National Crime Prevention Council Singapore. (2021b, June). *You don't need to be a mind reader to recognise a Credit-For-Sex scam. Just stay alert to the signs to...* [Video]. Facebook. https://www.facebook.com/ncpc.sg/videos/499704054782525/

National Crime Prevention Council Singapore. (2021c, June 3). *Scammers are always looking for ways to cheat our money. So, let's keep our eyes open to spot their tricks! [Photograph]*. Facebook. https://www.facebook.com/ncpc.sg/photos/a.146829248684077/4345093755524251/?type=3&theater

Nickerson, R. S. (1998). Confirmation bias: A ubiquitous phenomenon in many guises. *Review of General Psychology, 2*(2), 175-220. doi:10.1037/1089-2680.2.2.175

Norris, G., Brookes, A., & Dowell, D. (2019). The psychology of internet fraud victimisation: A systematic review. *Journal of Police and Criminal Psychology, 34*(3), 231-245. https://doi.org/10.1007/s11896-019-09334-5

Office for National Statistics. (2020, July 17). *Crime in England and Wales: year ending March 2020.* https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2020#fraud

Office for National Statistics. (2021, May 13). *Crime in England and Wales: year ending December 2020.* https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingdecember2020#fraud

Petty, R. E., & Cacioppo, J. T. (1986). The elaboration likelihood model of persuasion. Communication and Persuasion, 1-24. https://doi.org/10.1007/978-1-4612-4964-1_1

Reid, R. L. (1986). The psychology of the near miss. Journal of Gambling Behavior, 2(1), 32-39. doi:10.1007/bf01019932

Ross, L. (1977). The intuitive psychologist and his shortcomings: Distortions in the attribution process. *Advances in Experimental Social Psychology,* 173-220. doi:10.1016/s0065-2601(08)60357-3

REFERENCES

Ross, S., & Smith, R. G. (2011, August). Risk factors for advance fee fraud victimisation. *Trends and Issues in Crime and Criminal Justice*. https://core.ac.uk/download/pdf/30680737.pdf

Shadel, D., Pak, K. & Sauer, J. (2014, March). *Caught in the scammer's net: Risk factors that may lead to becoming an internet fraud victim, AARP survey of Florida adults age 18 and older.* AARP Research. Washington, DC. https://doi.org/10.26419/res.00076.004

Shover, N., Coffey, G. S., & Hobbs, D. (2003). Crime on the line. Telemarketing and the changing nature of professional crime. *British Journal of Criminology, 43*(3), 489-505. https://doi.org/10.1093/bjc/43.3.489

Singapore Police Force. (2020, August 26). Mid-year crime statistics for January to June 2020. https://www.police.gov.sg/-/media/EC2098477DD646738DE417936BFEFCFF.ashx

Singapore Police Force. (2021, August 30). In the first half of 2021, robbery, housebreaking, and snatch theft decreased by 40.5% collectively to 75 cases, down from ... [Photograph]. Facebook. https://www.facebook.com/56706929407/photos/a.449307704407/10161326633519408/

Singapore Police Force. (2021a, August 30). Mid-year crime statistics for January to June 2021. https://www.police.gov.sg/-/media/64A8EB6D3C8F45A2A762690BFA5B1400.ashx

Starcke, K., & Brand, M. (2016). Effects of stress on decisions under uncertainty: A meta-analysis. *Psychological Bulletin, 142*(9), 909.

Tan, D. (2021, March 01). *Committee of Supply debate 2021 on "Securing Singapore with the community"* [Speech transcript]. Ministry of Home Affairs. https://www.mha.gov.sg/mediaroom/parliamentary/committee-of-supply-debate-2021-on-securing-singapore-with-the-community-speech-by-mr-desmond-tan-minister-of-state-ministry-of-home-affairs-and-ministry-of-sustainability-and-the-environment/

Tan, T., & Kurohi, R. (2020, April 05). *Anxiety and worry amid Covid-19 uncertainty*. The Straits Times. https://www.straitstimes.com/singapore/anxiety-and-worry-amid-covid-19-uncertainty

Taylor, S. (2019). *The psychology of pandemics: Preparing for the next global outbreak of infectious disease*. Cambridge Scholars Publishing.

Titus, R. M., & Gover, A. R. (2001). Personal fraud: The victims and the scams. *Crime Prevention Studies, (12),* 133-152.

Trend Micro. (n.d.). *Cybercriminals - definition*. Trendmicro.com. https://www.trendmicro.com/vinfo/us/security/definition/cybercriminals

Wood, S., Hanoch, Y., & Woods, G. W. (2016). Cognitive factors to financial crime victimization. *Financial crimes: Psychological, technological, and ethical issues* (pp. 129-139). Springer.

Yeo, H. K., Ong, J., Chawla, A., Chai, X. T. W., & Khader, M. (2020). Behavioural practices of effective scammers: An Analysis of Scam Scripts (HTBSC Research Report 24/2020). Home Team Behavioural Sciences Centre.

You, J. K. & Imran, M. (2020, May 13). *Impact of COVID-19 on Financial Crimes* [PDF Slides]. Interpol. https://rm.coe.int/3148-2-2-28-webinar-5-online-fiscal-investigation-interpol/16809e548c

About Home Team Behavioural Sciences Centre

The Home Team Behavioural Sciences Centre (HTBSC) is a research and training outfit established in 2006 and based at the Home Team Academy. With the aim to enhance the operational effectiveness of Home Team (HT) officers, HTBSC emphasises the application of behavioural sciences principles into effective practices for law enforcement and emergency services. As a scientific response to evidence-based policies, HTBSC advocates the integration of research with ground operations to ensure HT officers stay relevant and fast-adapting to the ever-changing security landscape and challenges. Since its inception, the HTBSC has conducted research and training in three key areas (specialised branches):

1. Crime, Investigation and Forensic Psychology (CIFP)
2. Operations and Leadership Psychology (OLP)
3. Resilience, Safety and Security Psychology (RSSP)

in particular, the Crime, Investigation and Forensic Psychology (CIFP) branch of HTBSC oversees the development and implementation of investigative and forensic areas of the work of HTBSC. The CIFP branch applies knowledge from the field of forensic and investigative psychology to support officers in tackling operational challenges faced in the HT. Knowledge derived from CIFP research efforts informs training workshops and research forums/seminars, operational support initiatives and also security policies and investigative practices in the HT.

Since its formulation, CIFP's core area of work includes applying psychological principles in understanding and enhancing investigative support tools and initiatives in the following domains:

1. Behavioural Analysis of Violent and Sexual Crimes
2. Understanding Cyber & Emerging Crimes
3. Supporting HT Investigation and Operations through Investigative Interviewing & Intel Questioning
4. Embracing Technology in Psychology
5. Assessing Threat and Risk of Violence
6. Detecting Deception and Truth
7. Scam Prevention and Public Education

For more information, please contact Senior Assistant Director CIFP, Ms Whistine Chai at chai_xiau_ting@mha.gov.sg.

Editorial Board

Publisher	Home Team Behavioural Sciences Centre
Advisor	Dr Majeed Khader
Editors	Ms Whistine Chai Ms Siti Mariam Ms Vivian Seah
Contributors	Ms Whistine Chai Mr Joel Ong Ms Afreen Chawla Ms Joan Teo Ms Sabrina Lee

Acknowledgements

Special thanks to the following organisations and individuals who have supported the research or helped us with our book:

Consultation Panel

Singapore Police Force
Research and Statistics Division (MHA)
Policy Development Division (MHA)
Cyber Security Agency of Singapore
Lazada
Carousell
AXS Infocomm Pte Ltd
Alipay
United Overseas Bank
DBS Bank
Oversea-Chinese Banking Corporation Limited (OCBC Bank)
Dr Chia Yee Fei
Ms Sabrina Ng
Mr Richard Soh
Associate Professor Fred Long Foo Yee
Mr Ong Kian Chye
Assistant Professor Jiow Hee Jhee
Dr Natalie Pang Lee San
Dr Razwana Begum
Dr Emily Ortega
Associate Professor Denise Dillion
Associate Professor Jonathan Ramsay
Dr Chung Kai Li
Assistant Professor Olivia Choy
Associate Professor Krishna Savani
Associate Professor Elmie Nekmat

Office of Chief Psychologist

HTBSC
Ms Penelope Wang
Ms Stephanie Chan
Mr Karthigan Subramaniam
Ms Shannon Ng
Muhammad Azhiim

CAPS
Ms Diong Siew Maan
Ms Stephenie Wong
Ms Yeo Hui Kun

PPSD
Mr Jansen Ang
Ms Carolyn Misir
Ms Ho Hui Fen