中華警政研究學會

警政與警察法相關圓桌論壇(第 63 場)

【打擊詐騙系列座談(三)】紀錄

日期：2024 年 4 月 12 日 14:00

地點：網路視訊

主持人：詮理法律事務所 陳佳瑤所長

各位參與本次論壇的線上貴賓午安，今日舉辦「打擊詐騙」系列座談第三場，請到兩位引言人，第一位引言人是桃園市政府警察局外事科李堅志科長，他有多年駐外聯絡官的經驗，曾被派往泰國、印尼以及新加坡，破獲多起跨國重大刑案，曾獲得「外國駐印尼執法協會」(Indonesia Foreign Law Enforcement Community，IFLEC)頒發的貢獻獎，是第一位獲得這項殊榮的台灣警官，也是中國民國第 49 屆十大傑出青年，亦獲選刑事警察局「模範警察」。第二位引言人是中央警察大學行政警察學系許福生主任，他長年專注於少年犯罪、詐欺犯罪及刑事政策相關領域，在教學研究和實務方面都有豐富的經驗。引言發表結束之後，由銘傳大學犯罪防治學系章光明主任擔任評論總結，章主任專長為犯罪預防、警察政策及公共政策，現在也是本會的副理事長。論壇結束之前，會開放 20 分鐘綜合討論，線上的貴賓如果有提問或指教，都歡迎提出來分享。

詐騙犯罪確實已經成為一個全球性的問題。隨著科技的進步，詐騙者可以利用網絡和電子通訊工具在全球進行操作，這使得詐騙犯罪越來越難以防範和打擊，僅靠單一國家的努力往往難以應對這種跨國性的犯罪活動，因此國際合作是解決詐騙犯罪問題的關鍵之一。今日兩位引言人分別就新加坡及日本的詐騙犯罪情況進行介紹與分析，期望政府和社會各界共同努力，通過加強執法、加強合作以及提高公眾的警覺性和防範意識，來有效應對這一問題。

引言人 1：桃園市政府警察局外事科 李堅志科長

〈主題：新加坡打詐模式〉

〔**摘要**〕

一、前言

本文基於新加坡警察部隊於 2024 年 2 月 18 日發布的「2023 年新加坡刑事案件年報」與「2023 年新加坡詐欺及網路犯罪年報」，詳細介紹新加坡面臨的詐騙問題及其嚴重性，並探討當局如何透過修訂相關法令，企圖設法防治日趨嚴重的詐騙犯罪。

二、新加坡詐騙問題介紹

該部分將從詐騙數據、案件類型、財產損失和詐騙手法等方面進行分析，並探討針對新加坡人民詐騙犯罪的手法、工具及受害者類型。

三、新加坡打詐模式介紹

本節詳述新加坡政府在立法和政策層面如何應對詐騙問題，以及修法及新訂頒佈的《2023 網路犯罪危害法》等措施的實施情況，星國諸多做法頗值得我國借鏡，但仍應持續觀察其具體效果。

四、台星打詐合作機制

介紹自 2019 年以來，台灣和新加坡在打擊詐騙犯罪方面的合作機制，包括我國警政署派駐新加坡警察聯絡官的角色和台星兩國警方合作的具體成果。

五、結論

總結新加坡對詐騙犯罪的應對策略和立法措施，並強調國際合作在打擊跨國詐騙犯罪中的重要性。提出未來研究與合作的方向，以加強打詐效能和防範策略。

壹、前言

本文係依據新加坡警察部隊於 2024 年 2 月 18 日最新公布的新加坡刑事案件 2023 年報(Annual Crime Brief 2023 Physical Crime Situation)及新加坡詐欺及網路犯罪 2023 年報(Annual Scams and Cybercrime Brief 2023 Overall Scams and Cybercrime Situation)，介紹新加坡近年遭遇詐騙問題的嚴重性及星國當局所採行的因應政策。

本文同時將介紹星國政府針對該國內日益嚴重的詐欺犯罪問題，採取積極立法針對防制詐欺等網路犯罪危害的特別法---《網路犯罪危害法》(ONLINE CRIMINAL HARMS ACT 2023(No. 24 of 2023))，該法甫於 2023 年 7 月 5 日經國會立法通過並於同月 24 日經總統公布，並已於 2024 年 2 月 1 日正式生效。然而，該特別法能否如預期強化打詐效能，得否有效遏止詐騙案件持續發生，殊值各界觀察，而其後續成效更可做為我國打詐政策及研議立法的重要參考。

此外，本文目的透過介紹新加坡的詐騙犯罪問題現況及星國當局所採行的打詐政策，有效了解星國當局無論在立法及執法等層面均付出的努力及展現積極解決問題的企圖心。故本文共分三大部份：

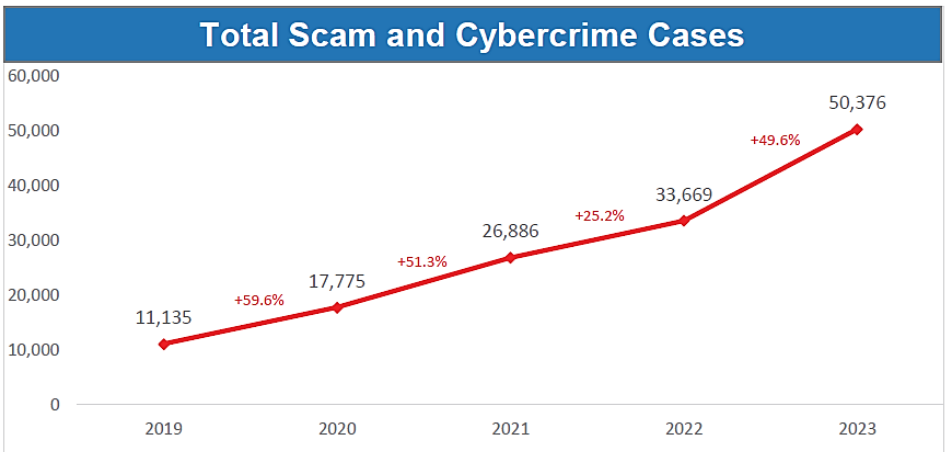
一、PART 1 新加坡詐騙問題介紹：分成詐騙數據、案類、財損(均以星幣為單位)、手法等細項分析及統計呈現；進而分析詐騙犯案工具及被害人類型等。

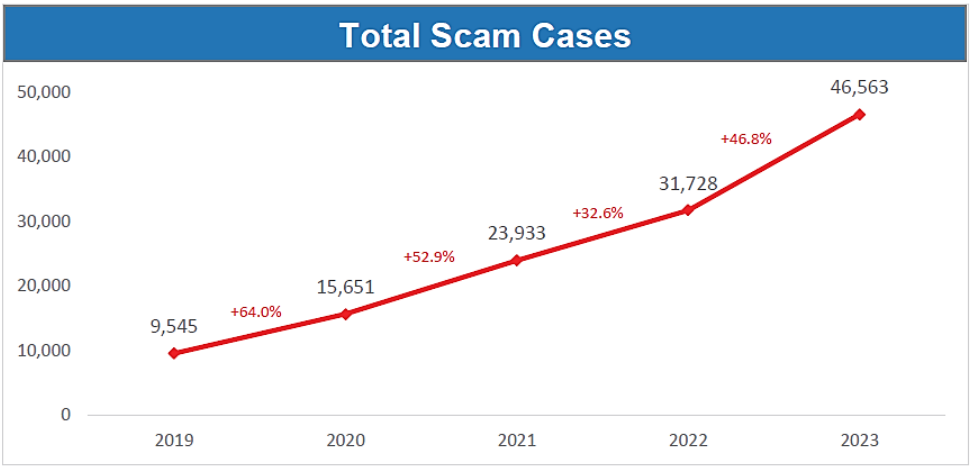
二、PART 2 新加坡打詐模式介紹：政府當局的打詐政策與成效，以及立法部門積極修訂刑法等相關法令並為強化打詐制定特別法---《網路犯罪危害法》

三、PART 3 臺星打詐合作機制為題，概略介紹我國警方自 2019 年 2 月 1 日起派遣首任駐新加坡警察聯絡官以來，對於台星兩國共同打擊詐欺犯罪建立合作機制，發揮務實功能且展現具體貢獻。

貳、新加坡詐騙問題介紹

在新加坡 2023 年報中，詐騙及網路罪案發生數由 2022 年的 33,669 宗上升 49.6%至 50,376 宗。其中，詐騙案件包括惡意軟體詐騙案在內，就佔這 50,376 起案件的 92.4%。詐騙案件總數由 2022 年的 31,728 宗增加 46.8%至 2023 年的 46,563 宗。





以下是新加坡前十大詐騙類型，又以排名前五的求職詐騙(job scams)、電子商務詐騙(e-commerce scams)、假朋友電話詐騙(fake friend call scams)、網路釣魚詐騙(phishing scams)和投資詐騙(investment scams)詐騙類型，危害最為嚴重。這些騙案佔 85.5%，約佔所有詐騙類型的 78.4%。

然而，2023 年前十大詐騙案類，冒充政府官員騙案(government officials impersonation scams(GOIS))則是平均損失最高的案類，每宗約 10 萬 3,600 元，其次是投資騙案，每宗約 5 萬 700 元。這兩種騙局類型涉及在一段時間內進行的欺騙和社會工程，使用一系列複雜的騙局方法。

Top 10 scam types in Singapore (Based on number of reported cases)

Types of Scams	Cases reported		Total amount lost (at least)		Average amount lost per case		
	2023	2022	2023	2022	2023	2022	Difference
Job Scam	9,914	6,492	$135.7M	$117.4M	$13,692	$18,089	↓ $4,397
E-commerce Scam	9,783	4,762	$13.9M	$21.3M	$1,428	$4,491	↓ $3,063
Fake Friend Call Scam	6,859	2,106	$23.1M	$8.8M	$3,373	$4,201	↓ $828
Phishing Scam	5,938	7,097	$14.2M	$16.5M	$2,394	$2,338	↑ $56
Investment Scam	4,030	3,108	$204.5M	$198.3M	$50,754	$63,834	↓ $13,080
Malware-enabled Scam	1,899	-	$34.1M	-	$17,960	-	-
Social Media Impersonation Scam	1,570	1,696	$9.7M	$3.7M	$6,184	$2,231	↑ $3,953
Loan Scam	914	1,031	$6.1M	$9.3M	$6,676	$9,082	↓ $2,406
Internet Love Scam	913	868	$39.8M	$35.7M	$43,677	$41,200	↑ $2,477
Government Officials Impersonation Scam	893	771	$92.5M	$97.6M	$103,657	$126,697	↓ $23,040
Top 10 scams	42,713	27,931	$573.9M	$509.2M	$13,438	$18,232	↓ $4,794

Note: Total amount lost may not tally due to rounding.

一、求職詐騙(job scams)

新加坡求職詐騙在2023年的舉報案件數量最多。2023 年報案9,914 例，而 2022 年為 6,492 例，增加了 52.7%。2023年造成的總損失從 2022 年的1.174 億元增加到1.357 億元，增長了 15.6%。2023年，每宗求職詐騙案件的平均損失金額從2022年的18,089元下降24.3%至13,692美元。工作詐騙通常涉及向受害者提供可以在家中完

成的在線工作。他們將被要求執行傭金任務，例如提前購買、喜歡社交媒體帖子、評論酒店/餐館/航空公司、完成調查、“提升”加密貨幣的價值、“提升”在線商家產品清單的評級，或“評級”移動應用程式以提高他們在應用商店的排名。提供給受害者的另一項「工作」需要將資金轉移到詐騙者提供的銀行帳戶，收取少量傭金。詐騙者隨後會要求轉移更多資金，據稱是為了獲得更高的收入。受害者最終會意識到，當他們未能收到傭金時，當他們無法從銀行帳戶中提取資金時，或者當他們無法再聯繫到詐騙者時，他們被騙了。

在其他情況下，詐騙者會在網上與受害者交朋友，並尋求兼職工作的說明或提供賺錢的機會。受害者將獲得電子商務網站，並被要求截取特定產品，並向虛假的“企業帳戶”支付預付款，以獲得傭金並承諾退款。這個過程會重複幾次，從低成本的專案開始，然後再發展到更昂貴的專案。受害者最初會收到傭金和退款，但詐騙者最終會聲稱遇到了問題，並在無法聯繫到之前停止“支付”受害者。大多數求職詐騙受害者年齡在30至49歲之間，占該類詐騙受害者的45.4%。詐騙者用來聯繫工作詐騙受害者的最常見平臺是 WhatsApp 和 Telegram。

二、電子商務詐騙（e-commerce scams）

電子商務詐騙在新加坡所有詐騙類型中報告的案件數量位居第二。2023 年報告了 9,783 案例，而 2022 年為 4,762 例，增加了 105.4%。2023年，電子商務詐騙造成的總損失從 2022 年的至少 2,130 萬元下降至 1,390 萬元，下降了 34.7%。每宗電商騙案的平均損失金額由2022年的$4,491下降至2023年的$1,428，跌幅為68.2%。ii. 電子商務詐騙涉及在沒有實體聚會的情況下銷售商品和服務。一般來說，受害者會在在線市場或社交媒體平臺上遇到有吸引力的交易，但在付款后無法收到商品或服務。在某些情況下，受害者是賣家，他們在將商品或服務交付給冒充買家稱沒有收到付款。詐騙者有時會向受害者提供虛假截圖作為「付款證明」(proof of payment)。

2023 年出現的一種新的電子商務詐騙變種涉及免費回收利用(freecycling)，受害者在社交媒體平臺上看到提供免費贈品或以折扣價出售商品的帖子。當詐騙者要求支付商譽押金、預訂費或付款時，受害者遭受了經濟損失。iv. 電商詐騙案件中常見的物品包括住宅租賃、電子產品和演唱會門票。v. 大多數電子商務詐騙受害者年齡在30至49歲之間，占該類詐騙受害者的49.3%。進行電子商務詐騙的最常見平臺包括Facebook、Carousell和Telegram。詳參各平臺的電商騙案明細。

三、假交友電話詐騙(fake friend call scams)

2023年有6,859宗假朋友電話詐騙案件，而2022年為2,106宗，增加了225.7%。2023年，虛假朋友電話詐騙造成的損失總額從2022年的至少880萬星幣增加到至少2310萬元，增長了162.5%。2022年，每次假朋友電話詐騙的平均損失金額從 2022 年的 4,201 元下降到 3,373 元，下降了 19.7%。

假交友電話詐騙通常涉及詐騙者通過電話或 WhatsApp 與受害者聯繫，假裝是他們的熟人。在談話過程中，詐騙者會聲稱他們丟失了手機並更換了電話號碼。在建立融洽的關係后，騙子會利用感知到的友誼，以各種理由向受害者索要錢財。騙子為這

些「貸款」提供的常見原因是向承包商支付裝修費、支付與開設新業務相關的費用或向供應商/供應商付款。受害者會通過PayNow將錢轉入屬於不知名人士的銀行帳戶。當他們聯繫他們的實際熟人時，他們會發現自己被騙了，並意識到他們既沒有更改聯繫電話也沒有聯繫他們。受害者大部分年齡在50至64歲之間，占該類詐騙受害者的37.5%。電話和 WhatsApp 是假朋友電話詐騙者聯繫潛在受害者的最常見管道。

四 、網络釣魚詐騙(phishing scams)

2023 年共發生 5,938 起網路釣魚詐騙案件，而 2022 年為 7,097 起，下降了16.3%。網路釣魚詐騙造成的損失總額也從 2022 年的至少 1650 萬元下降到 2023 年的至少 1420 萬元，下降了 13.9%。2023年，每宗網路釣魚詐騙案件的平均損失金額從 2022 年的 2,338元略微增加 2.4% 至 2,394 元。

網路釣魚詐騙涉及詐騙者冒充政府官員、金融機構或企業發送的電子郵件、消息、電話或廣告。受害者會被誘騙通過點擊惡意連結或電話洩露敏感資訊，例如使用者名、密碼、銀行憑證和/或轉帳卡或信用卡資訊。騙徒在取得受害人的資料后，會利用受害人的銀行帳戶或轉帳卡/信用卡進行未經授權的交易。網路釣魚詐騙變種包括詐騙者的以下行為：·通過市場平臺冒充感興趣的買家，詐騙者會冒充潛在買家，並通過對 Carousell 等在線市場平臺上列出的待售商品表示興趣來接近受害者。受害人會以收取貨款或支付快遞服務為藉口，通過電子郵件或應用內消息收到惡意 URL 連結或二維碼，以方便運送物品。點擊惡意連結后，受害者被引導至欺騙性的銀行或快遞公司網站，提示受害者輸入他們的銀行憑據、轉帳卡/信用卡詳細資訊和一次性密碼(One-Time-Passwords (OTPs))。通過電話冒充政府官員，受害者會收到據稱來自新加坡警察部隊SPF和人力部(the Ministry of Manpower (MOM))等政府官員的不請自來的電話或應用程式內電話。

新加坡大多數網路釣魚詐騙受害者年齡在30至49歲之間，占該類詐騙受害者的47.8%。輪播、簡訊和Facebook是網路釣魚詐騙者聯繫潛在受害者的最常見管道。

五、投資詐騙（investment scams）

2023年發生4,030宗投資詐騙個案，較2022年的3,108宗增加29.7%。2023年，投資詐騙造成的總損失從2022年的至少1.983億元增加到至少2.045億元，增長了3.1%。在十大騙局類型中，投資騙局的損失最高，儘管每宗投資騙局的平均損失金額從2022年的63,834元下降到2023年的50,754元，但損失金額最高。

受害人通過WhatsApp和Telegram等消息平臺被添加到聊天組或頻道的案件呈上升趨勢，據稱是為了“投資機會”。在這些聊天組或頻道中，受害者收到了來自其他成員的多項索賠，這些成員從他們的投資中“獲利”，使受害者相信投資的真實性。在承諾的回報的誘惑下，受害者會聯繫騙子。然後，他們會與騙子分享個人資訊，以「開立帳戶」並轉移資金進行“投資”。在收到「投資」收益之前，騙子指示受害者轉移資金以支付「投資」產生的各種費用」。受害人會意識到，儘管他們支付了“投資”的“費用”，但仍無法提取“利潤”，他們就會意識到自己被騙。

投資騙案受害人年齡介乎30至49歲，占該類騙案受騙受害人的45.1%。Facebook、Telegram 和 Instagram 是投資詐騙者聯繫潛在受害者的最常見平臺。惡

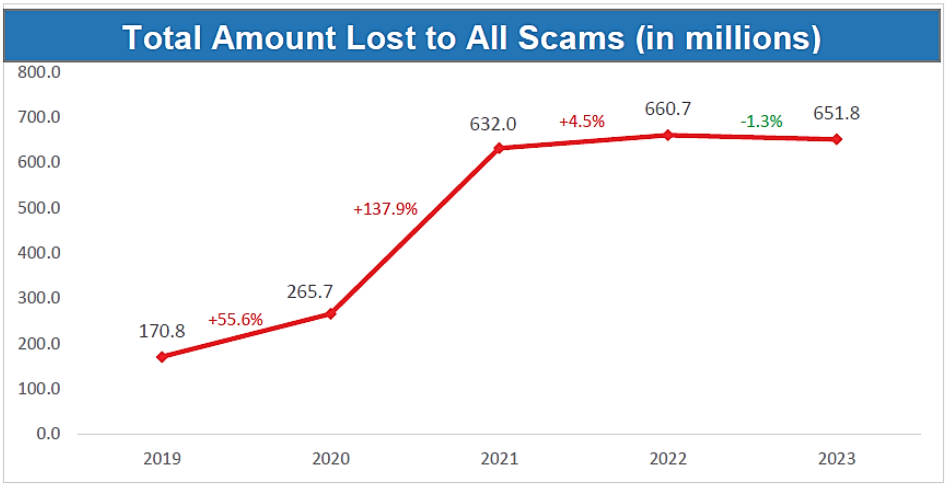
意軟體詐騙 10.在2023年，大約有1,899宗受害人將惡意軟體下載到手機上的案件，損失總額至少為3,410萬元。每個支援惡意軟體的詐騙案件的平均損失金額約為17,960元。

受害人一般會回應Facebook及Instagram等社交媒體平臺上的服務廣告（例如家居清潔、購買食物及寵物美容）。詐騙者會以支付服務費用為藉口，通過WhatsApp向受害者發送檔或URL連結，要求他們下載Android Package Kit（APK）檔，這是為Android操作系統創建的應用程式。這些APK檔包含針對受害者設備的惡意軟體。受害人下載APK檔后，騙徒可能會指示受害人向類似於銀行登錄網站的欺騙網站提供他們的銀行憑證和/或銀行卡詳細資訊來付款。該惡意軟體還可能允許詐騙者遠端訪問受害者的設備。這將允許詐騙者通過鍵盤記錄或監控受害者對其設備的使用方式來獲取受害者的銀行憑證和/或銀行卡詳細資訊。隨後，受害者在討論時會意識到他們被騙。

大多數啟用惡意軟體的詐騙受害者年齡在 30 至 49 歲之間，占此類詐騙類型受害者的 43.7%。Facebook 和 Instagram 是詐騙者用來聯繫潛在受害者的最常見平臺。iii. 為應對惡意軟體詐騙攻擊，政府推出了一系列保護新加坡人的措施，導致 2023 年底的病例有所下降。全政府（WOG）的反惡意軟體詐騙措施包括加強措施，以保障中央公積金(Central Provident Fund (CPF))的款項、發佈安全應用程式標準（the Safe App Standard）以及與銀行合作推出反惡意軟體詐騙措施（counter malwareenabled scams measures）。

六、小結

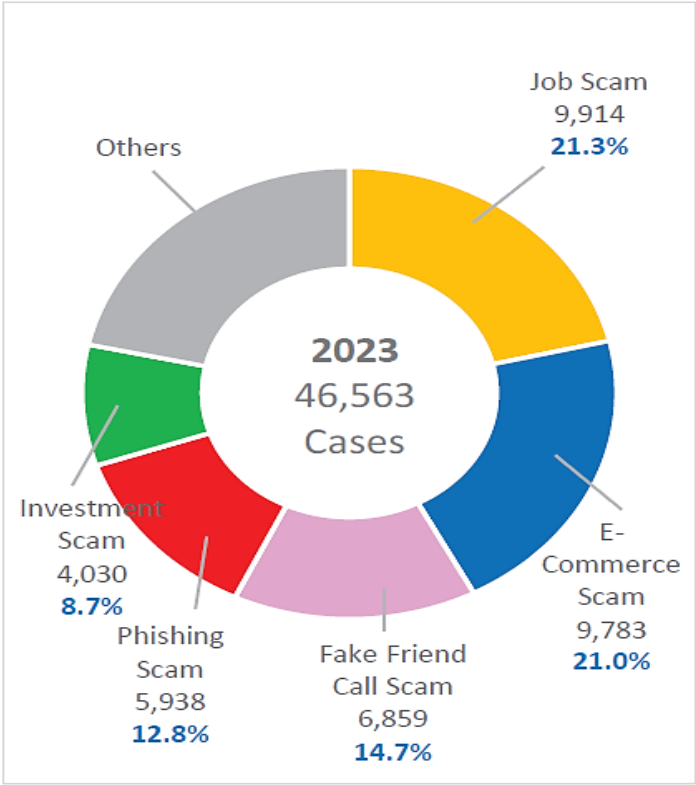
綜上，儘管新加坡詐騙個案數目有所增加，但2023年的損失總額由2022年的6億6070萬元微跌1.3%至6億5180萬元。這是過去五年來新加坡因詐騙而損失的總金額首次下降。



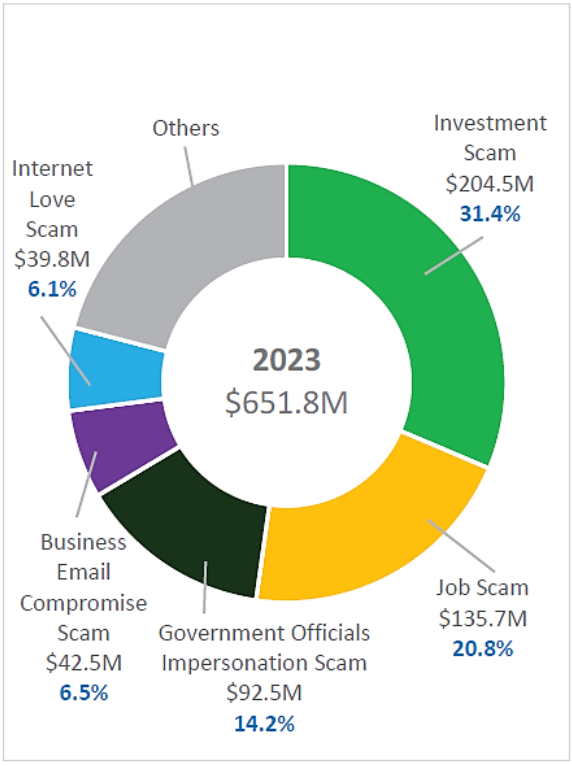
求職詐騙(job scams)、電子商務詐騙(e-commerce scams)、假朋友電話詐騙(fake friend call scams)、網路釣魚詐騙(phishing scams)和投資詐騙(investment scams)這五大詐騙類型的平均損失金額普遍下降。整體而言，所有已報案的每宗詐騙個案的平均損失金額亦有所下降，由2022年的20,824元下降至2023年的13,999元，跌

幅約32.8%。

Breakdown of scam types by number of cases



Breakdown of scam types in terms of amount lost (in millions)



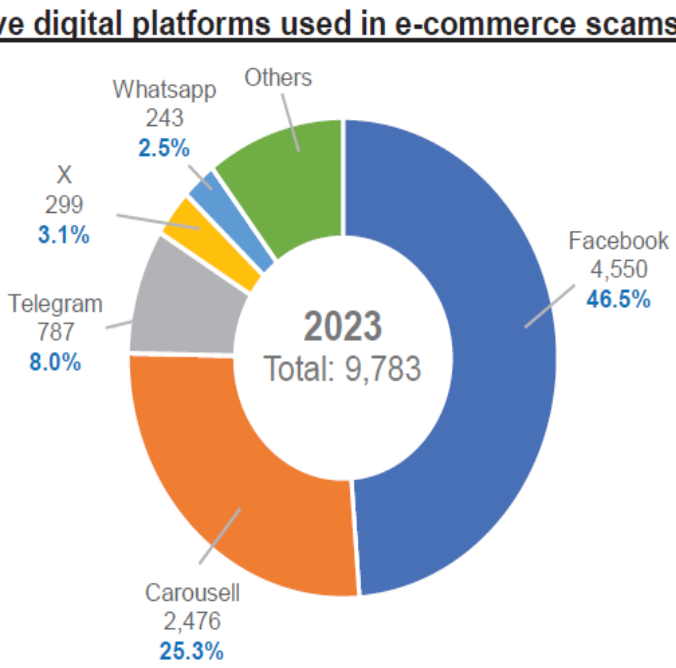
損失略有改善的部分原因可能是新加坡警察部隊 （SPF）、資訊通信媒體發展局

(Infocomm Media Development Authority (IMDA))、新加坡網路安全域 (Cyber Security Agency of Singapore (CSA))、智慧國家集團(Smart Nation Group (SNG))、新加坡金融管理局(Monetary Authority of Singapore (MAS))和私人安全利益相關者(private sector stakeholders)為防止詐騙並阻止或減輕正在進行的詐騙期間的損失而做出的積極和協調努力，以及提高公眾對個人可以採取的措施的認識，以避免被騙。

然而，涉及使用社會工程和欺騙手段誘使受害人將錢款轉給騙徒的騙局損失仍然很高。通過社交媒體和消息平臺（如Facebook、Instagram、WhatsApp和Telegram）實施的詐騙數量急劇增加感到擔憂。個人保持警惕仍然至關重要。通過隨時了解情況並謹慎行事，每個人都可以更好地保護自己和彼此免受詐騙。

七、新加坡詐騙工具及方式

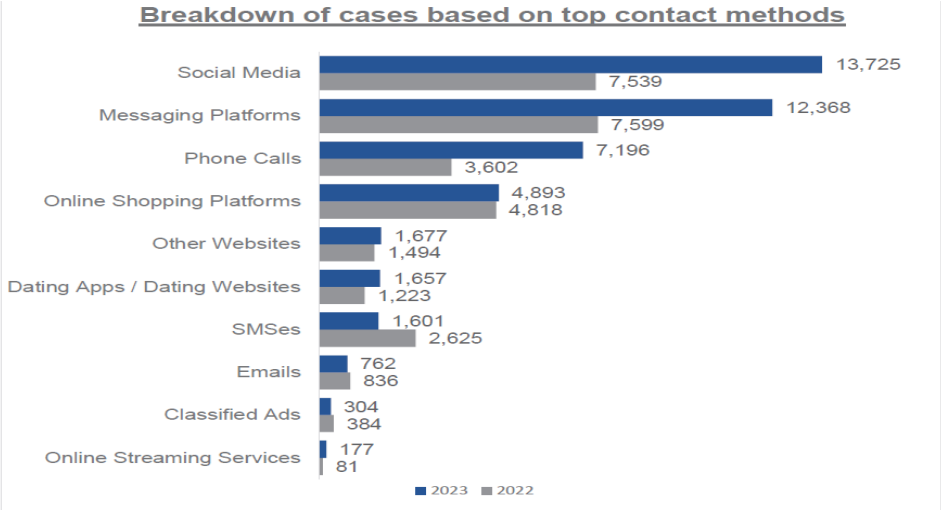
(一)詐騙者傾向於通過社交媒體、消息平臺、電話、在線購物平臺和其他網站等五種接觸方式與受害者聯繫。

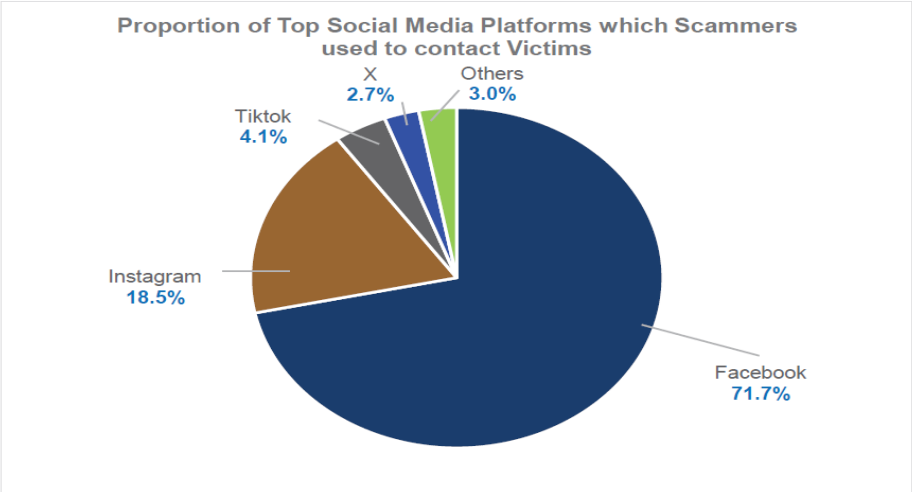


(二)Meta的三款產品—Facebook、WhatsApp 和 Instagram——尤其值得關注，並且在詐騙者用來聯繫潛在受害者並進行詐騙的平臺中繼續佔比過高。有關Meta平臺上五大騙局的個案分析。

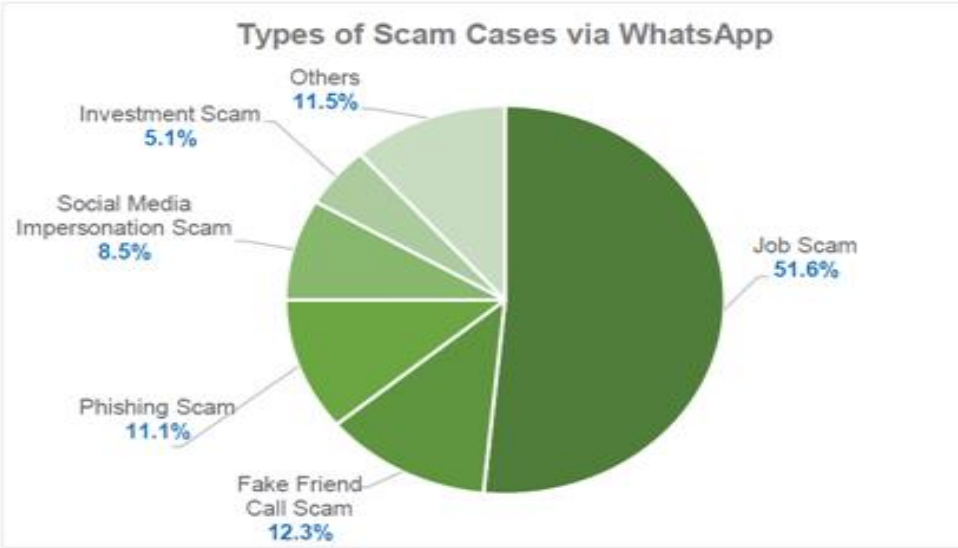
(1)2023年，騙徒通過社交媒體聯繫受害人的詐騙個案由2022年的7,539宗增加至13,725宗，其中Facebook約佔71.7%，Instagram佔18.5%。透過Facebook與受害人聯繫的騙案中，41.5%為電商詐騙，15.8%為惡意軟體詐騙，12.0%為求職詐騙。騙徒透過訊息平台聯繫受害人的詐騙個案由2022年的7,599宗增至2023年的12,368宗，其中約68.0%的個案通過WhatsApp，26.5%的個案透過Telegram。

Annex B.





(2)透過WhatsApp聯絡受害人的騙案中，51.6%為求職騙案，12.3%為假友詐騙案，11.1%為偽騙案。17. 另一種令人擔憂的聯繫方式是電話。2023年，通過電話進行的詐騙案件數量從2022年的3,602宗增加到7,196宗。其中，79.2%為假朋友詐騙，10.3%為冒充政府官員詐騙，2.9%為求職詐騙。



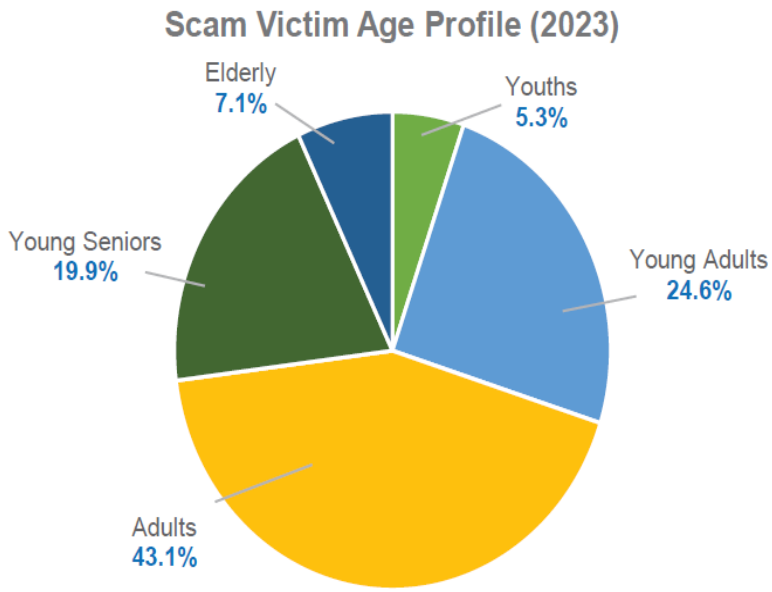
詐騙受害者剖繪

a）18.73.0%的騙案受害人為青少年、青年及 50 歲以下成年人。按年齡組劃分的騙案受害人分項如下： a） 19 歲及以下的青少年佔受騙受害人的 5.3%。這個年齡段的人中有 32.0%成為電子商務詐騙的犧牲品，而 25.4%的人成為工作詐騙的犧牲品，16.6%的人成為網路釣魚詐騙的犧牲品。詐騙者傾向於通過消息傳遞平臺、在線購物平臺和社交媒體聯繫年輕人。

b） 20 至 29 歲的年輕人占詐騙受害者的 24.6%。這個年齡段的人中有 31.9%成為工作詐騙的犧牲品，而 25.9%的人成為電子商務詐騙的犧牲品，10.6%的人成為網路釣魚詐騙的犧牲品。詐騙者傾向於通過消息平臺、社交媒體和在線購物平臺聯繫年輕人。.

c） 30 至 49 歲的成年人占詐騙受害者的 43.1%。24.6%的人成為電子商務詐騙的犧牲品，而 22.3%的人成為工作詐騙的犧牲品，14.3%的人成為網路釣魚詐騙的犧牲品。詐騙者傾向於通過社交媒體、消息平臺和在線購物平台聯繫這個受害者群體。

d） 50 至 64 歲的年輕老年人占詐騙受害者的 19.9%。28.0%的人成為虛假朋友電話詐騙的犧牲品，而 12.8%的人成為電子商務詐騙的犧牲品，12.2%的人成為網路釣魚詐騙的犧牲品。詐騙者傾向於通過社交媒體、電話和消息傳遞平台聯繫這個受害者群體。e） 65 歲及以上的長者占騙案受害人的 7.1%。這個年齡段的人中有 34.3%成為假朋友電話詐騙的犧牲品，而 13.7%的人成為投資詐騙的犧牲品，11.7%的人成為網路釣魚詐騙的犧牲品。詐騙者傾向於通過電話、社交媒體和消息平臺與老年人聯繫。



參、新加坡打詐模式介紹

有關新加坡針對打擊詐騙犯罪，**通過**修訂相關條文、罰則及特點以及新制定特別法「網路犯罪危害法」的方式，簡介如下：

一、星國修訂相關詐騙法令：

(一)刑法（Penal Code）第17章財產犯罪－詐騙（Cheating）：

1、條文：第 415 條至第 420 條

2、目的：處理詐騙相關犯罪行為。

3、處罰：依據具體罪行的性質，刑罰可能包括最高 1 年至 7 年有期徒期、罰金或兩者併科。

(二)刑法（Penal Code）第17章財產犯罪－不實收受贓物（Dishonestly receiving stolen property）：

1、條文：第 411 條

2、目的：處理收受贓物相關犯罪行為（針對車手）。

3、處罰：可處 6 個月以上、5 年以下有期徒刑，或科或併科罰金。

(三)電腦濫用法（Computer Misuse Act）

1、條文：第 3 條及第 4 條

2、目的：處理與電腦相關的罪行，包括駭客入侵、身份盜竊及網路詐騙等。

3、處罰：相關犯罪行為得科以最長 20 年有期徒刑及/或罰金。

4、說明：電腦濫用法（CMA）配合腐敗、毒品販運及其他嚴重罪行（沒收收益）法（CDSA）於 2023 年 5 月進行修訂，使新加坡警方能夠更有效地對付錢騾(Money mule)和那些濫用 Singpass 進行犯罪活動的人。CDSA 新增了一些罪行，令警方更容易認定要件構成洗錢罪，而 CMA 的修訂則允許警方得以處置濫用 Singpass 憑證的個人。新修訂條款於甫 2024 年 2 月 8 日生效。

(四)消費者保護（公平交易）法（Consumer Protection Act）：

1、目的：保護消費者免受詐欺及不公平交易行為、誤導性廣告與詐騙性銷售策略的侵害。

2、處罰：相關違法行為可處以罰款、有期徒刑及對被害人的賠償等懲罰。

(五)直銷和金字塔銷售（禁止）法（Direct Selling and Pyramid Selling Act）：

1、目的：管理多層次行銷（MLM）與金字塔銷售計畫，確保它們合法透明地運作。

2、處罰：參與非法的 MLM 或金字塔騙局可處以罰金、有期徒刑或兩者併科。

二、新頒「網路犯罪危害法」（Online Criminal Harms Act）。

該法係新加坡政府甫於 2023 年 7 月通過的新法案，經國會審議通過，並於 7 月 24 日經總統同意後頒布，且已於 2024 年 2 月 1 日實施生效，訂定此法目的在於讓政府可以更有效地應對現代具犯罪性質的網路活動，相關特點如下：

(一)針對特定違法犯罪的政府指令：

1、該法案將允許政府向任何可能進行犯罪活動的網路服務發布「指令」（Direction），並適用於法案規定的特定刑案類型，例如：影響國家安全、國家和諧及個人安全的犯罪。

2、當合理懷疑（when there is reasonable suspicion）某些網路行為正在從事犯罪活動時，可依據犯罪事實發布以下相關指令：

(1)停止通訊指令（Stop Communication Direction）：要求指令的接收者停止向新加坡民眾傳播特定的網路內容（包括本質相似的內容）。指令的接收者可以是傳達此類網路內容的個人及實體。

(2)內容屏蔽指令（Disabling Direction）：要求提供網路服務業者屏蔽其服務中的特定內容（如：發文或網頁），其中可能包含相同內容的副本。

(3)帳戶限制指令（Account Restriction Direction）：要求提供網路服務業者停止使用其服務的帳戶在新加坡進行通訊和/或與新加坡民眾聯繫。

(4)網路屏蔽指令（Access Blocking Direction）：要求提供網路服務業者阻止新加坡民眾訪問特定網路位置。

(5)應用程式下架指令（App Removal Direction）：要求應用程式廠商從其新加坡頁面中刪除指定應用程式，避免新加坡民眾繼續下載該程式。

(二)主動預防詐騙及惡意網路活動：允許政府在懷疑（when it is suspected）任何網站、網路帳戶或網路活動可能被用於詐騙或惡意網路活動時發布指令。與其他特定的刑事犯罪相比，採取較低的行動門檻能使政府能在任何人成為受害者之前，阻止詐騙及惡意網路活動。

(三)警方可以依據該法要求指定的線上服務實施系統、流程或措施來對抗詐騙，例如要求用戶身份與政府頒發的身份證件進行驗證。

三、打詐行政措施

(一)警方成立「反詐騙指揮處」（Anti-Scam Command，ASCom）

新加坡警察部隊（SPF）於 2021 年 3 月 22 日將商業事務局（CAD）下的反詐科（Anti-Scam Division）提升為「反詐騙指揮處」（ASCom）。如同我國刑事警察局的打詐中心及 165 專線(星國是 1800-722-6688)，ASCom 旨在整合 SPF 內不同的反詐騙單位，將詐騙調查、事件處理、介入、執法與情報分析功能統一管理。該指揮處包括反詐騙中心（Anti-Scam Centre，ASC）、3 個反詐騙調查組，並督導 7 個地區警署內的打詐小組。

ASCom 著重於打擊詐騙集團上游活動，以阻斷歹徒的施詐行為，並利用科技及自身技術強化其情報分析能力。此外，該指揮部還與超過 90 個機構合作打擊詐騙。這些機構包括本地及外國銀行、卡片安全組織、非銀行金融機構（例如Grab、Singtel DASH）、通訊業者、金融科技公司及加密貨幣平台（如 Wise、Xfers Pte Ltd 和 Coinhako），以及新加坡的匯款服務業者等。透過建立直接通訊管道及緊密的工作關係，達到迅速凍結帳戶、追回款項，減少被害人損失之目標。

(二)推動發送簡訊ID實名註冊制（SMS Sender ID Registry，SSIR）

新加坡資訊通訊媒體發展局（Info-Communications Media Development Authority）針對預防電信詐欺犯罪問題，為強化保護 SMS 簡訊通訊管道，避免其淪為詐騙集團之犯罪工具。自 2022 年 1 月 31 日起，規定所有發送群體簡訊的組織都需要在「新加坡簡訊發送者 ID 名單」（SSIR）進行註冊，目的在於強化對發送 SMS 簡訊的管控。任何未經註冊的組織所發送之簡訊將被標記為「可能是詐騙」（Likely-SCAM），此與垃圾郵件過濾器及垃圾郵件箱的功能類似。藉以提醒民眾收到未註冊簡訊時，應特別小心該簡訊上資訊的真實性。

(三)研發「ScamShield」反詐應用程式（App）

新加坡「國家犯罪預防委員會」（National Crime Prevention Council）與「政府科技局」（Government Technology Agency）「政府公開產品」（Open

Government Products）部門，以及 SPF 合作開發官方的「ScamShield」反詐應用程式，並於 2020 年 11 月 20 日推出。目的在幫助使用者識別及封鎖詐騙來電與簡訊、檢舉詐騙案件，並及時了解最新的詐騙趨勢。

該應用程式包含「詐騙來電偵測」、「詐騙簡訊過濾」、「即時詐騙警報」、「檢舉詐騙」及「來電阻擋與個人封鎖清單」等功能，自上線以來，迄今已被用戶下載超過 60 萬次、超過 740 萬則簡訊被檢舉為潛在詐騙訊息，並封鎖了超過 7 萬個涉及詐騙的電話號碼。

(四)新加坡金融管理局推動反詐騙措施

鑑於警方日前與銀行密切合作追回贓款的經驗，ASCom 遂和新加坡金融管理局（MAS）與各家銀行合作，邀請各銀行指派其員工入駐在 ASCom 場所內（註：此處無涉法律規範)。自 2021 年 7 月 25 日起，星展銀行（DBS)、華僑銀行（OCBC)、大華銀行（UOB)、渣打銀行（SCB)、匯豐銀行（HSBC）和聯昌國際（CIMB）等六家新加坡主要銀行已響應派員進駐反詐中心的陣容，積極加強與警方的即時協調以進行調查工作、追查資金流向以及凍結涉嫌涉案的銀行帳戶。ASCom 於 2021 總計凍結了超過 16,700 個合作銀行帳戶，並追回約星幣 1 億 4660 萬元，追回率超過 60%。此成效顯示與銀行同地辦公著實強化新加坡警方的打擊詐騙工作。

MAS 繼續與新加坡銀行協會的常設反欺詐委員會緊密合作，打擊數字銀行詐騙。為了打擊通過惡意軟體控制客戶設備和移動銀行訪問權的詐騙，並保護客戶免受惡意軟體的侵害，MAS 與 SPF 合作，與銀行一起實施了防範措施。從 2023 年 8 月開始，各銀行逐步推出了升級版的銀行應用，配備了反惡意軟體措施。這些措施限制了如果檢測到 Android 設備安裝了具有協助工具許可權的協力廠商應用，則無法訪問銀行應用。此後，隨著越來越多人升級了他們的銀行應用，惡意軟體啟動的詐騙案件開始顯著下降。與私營部門合作開發上游措施，直接促成了 2023 年末惡意軟體啟動的詐騙案件的減少。

在 2023 年 11 月，本地銀行推出了資金鎖定功能，該功能通過允許客戶在銀行帳戶中劃出一部分資金，不能進行數位轉帳，從而降低詐騙的影響。截至 2024 年 1 月，已設置了超過 49,000 個資金鎖定帳戶，劃出的資金超過 42 億美元。其他主要零售銀行將逐步推出資金鎖定功能，預計到 2024 年 6 月。銀行將繼續完善其反詐騙措施，並隨著威脅環境的變化，提高客戶對警示標誌的認識。

(五)新加坡資訊通信媒體發展管理局（IMDA）與電信公司合作實施反詐騙措施，作為多層防護措施的一部分，IMDA與電信公司合作，實施了加強對新加坡使用者短信和電話來電的保護的反詐騙措施。這包括允許用戶在其行動電話上遮罩來自國際號碼的來電，以及短信發送者ID註冊系統，其中未註冊的發送者ID將被標記為“可能是詐騙”，以警告用戶。

電信公司將限制每位訂戶的後付費 SIM 卡數量，為了防範本地 SIM 卡的非法使用，目前每個個人只允許購買最多三張預付費 SIM 卡，這足以滿足主要是外國訪客、遊客和合同工人的真實用戶的需求。SPF 和 IMDA 發現，由本地人購買的後付費 SIM 卡日益被用於詐騙。因此，將對個人限制購買最多 10 張後付費 SIM 卡。這個較高的上限是為了滿足合法用戶為家庭成員註冊 SIM 卡的需求，同時限制非法使用。

這項措施將於 2024 年 4 月 15 日生效，僅適用於新註冊。目前擁有超過 10 張

後付費 SIM 卡的用戶將不受影響。然而，他們將無法註冊更多 SIM 卡。IMDA 將隨時間審查後付費 SIM 卡的限制，以確保其持續相關性。

(六)促使銀行及電子商務平臺派員進駐反詐中心

鑑於警方日前與銀行密切合作追回贓款的經驗，ASCom 遂和新加坡金融管理局（MAS）與各家銀行合作，邀請各銀行指派其員工入駐在 ASCom 場所內（註：此處無涉法律規範)。自 2021 年 7 月 25 日起，星展銀行（DBS)、華僑銀行（OCBC)、大華銀行（UOB)、渣打銀行（SCB)、匯豐銀行（HSBC）和聯昌國際（CIMB）等六家新加坡主要銀行已響應派員進駐反詐中心的陣容，積極加強與警方的即時協調以進行調查工作、追查資金流向以及凍結涉嫌涉案的銀行帳戶。ASCom 於 2021 總計凍結了超過 16,700 個合作銀行帳戶，並追回約星幣 1 億 4660 萬元，追回率超過 60%。此成效顯示與銀行同地辦公著實強化新加坡警方的打擊詐騙工作。

四、警察嚴格執法強力取締

(一)執法掃蕩相關詐騙非法產業2023年，新加坡警方在全島範圍內進行了四次行動，針對17間手機店，並拘捕了11名涉嫌利用他人資料騙取SIM卡的人士。據稱，他們幫助詐騙者利用預先註冊的預付費/后付費SIM卡作為其非法活動的匿名通信管道。這四項行動導致3 000多條電話線被終止。

(二)ASC亦與本地電訊公司和電子商貿平臺）緊密合作，打擊用於詐騙的管道。2023年，超過9,200條據信用於詐騙的移動線路和超過29,200條 WhatsApp 線路被提交終止。此外，超過4,100個受詐騙污染的在線綽號和廣告被提交給各自的平臺進行刪除。

(三)2023 年 7 月，新加坡警方促成Coogle Cloud Priority Flagger 計劃，該計劃旨在加速識別和標記該服務上託管的潛在網路釣魚網站和惡意軟體。作為優先舉報人，SPF 提交的惡意網站和惡意軟體將被Google優先處理。SPF 還一直在與包括 Google 在內的在線平臺合作，引入更強有力的保護措施，以降低欺詐性接管在線消息帳戶的風險，例如通過先發制人的檢測和阻止連結到網路釣魚網站的 URL 阻止詐騙網站 28.SPF 使用分析工具來識別和阻止詐騙網站。2023年，SPF 與本地互聯網服務提供者合作，攔截了超過 25,000 個詐騙網站。

(四)由於大多數在線詐騙都是由新加坡境外的詐騙者實施的。此類案件難以調查和起訴。星國執法部門要成功偵破這些案件，有賴於海外執法機構的合作程度，以及他們在轄區內追查詐騙者的能力。這些騙子通常是有組織犯罪集團的一部分，他們從事複雜的跨國行動，不容易被發現或拆除。要追迴轉入新加坡境外的款項非常困難。儘管如此，SPF繼續與馬來西亞皇家員警和國際刑警組織等外國同行和合作夥伴密切合作，以交換資訊並開展聯合調查和打擊跨國詐騙的行動。2023年，新加坡警方與海外執法機構緊密合作，成功取締19個詐騙集團，包括8個工作詐騙及洗黑錢集團、6個假朋友電話詐騙集團、3個網路釣魚詐騙集團及2個互聯網愛情詐騙集團。拘捕超過110名海外人士，涉及730多宗詐騙案件。

五、提升全民預防詐騙能力

(一)自動化打擊詐騙策略和外展：除了執法外，ASCom還進行了上游干預，以識別和警

告受害者，並利用技術加強其意義形成能力。通過“自動化打擊詐騙策略和外展(Automation of Scamfighting Tactics & Reaching Out’（A.S.T.R.O.）)項目，ASCom與多家銀行合作，如OCBC、UOB和DBS，自動化資訊共用、資訊處理以及大量向詐騙受害者發送短信警報。許多受害者在收到警方的短信警告後，才意識到自己已經上當，被勸告立即停止任何進一步的金錢轉帳。通過六次聯合行動，於2023年發送了超過68,000條短信，警告超過28,500名受害者。這種主動的做法避免了超過1.48億美元的潛在損失。

(二)預防性干預潛在詐騙受害者：為了加強SPF在社區預防詐騙方面的影響力，ASCom和警察局區警務部門共同對潛在詐騙受害者進行預防性干預。這些受害者是由銀行轉介的，因為他們被發現試圖進行可疑的金錢轉帳。在2023年，ASCom成功進行了590多次干預，為這些受害者進一步避免了超過4400萬美元的潛在損失。

(三)設立專門部門進行詐騙公眾教育：SPF於2023年設立了詐騙公眾教育辦公室（SPEO），推動反詐騙公共教育和意識提升工作。SPEO通過以下方式繼續擴大政府在詐騙問題上的外展工作：(1) 廣泛的專案和溝通；(2) 針對不同人群的目標化專案；及(3) 動員社區共同創造和宣傳反詐騙資訊和專案。通過各種平臺提供反詐騙資訊和資源為了教育公眾反詐騙保護措施，SPF繼續與全國犯罪預防理事會（NCPC）密切合作，推出“我可以對抗詐騙”活動。這次活動的視頻包含了一首特別創作的歌曲，鼓勵人們對抗詐騙。自2023年11月上傳至NCPC的YouTube頻道以來，該視頻已被觀看超過一百萬次。

(四)定期傳播最新和流行的詐騙類型資訊：SPF確保及時傳播最新和流行的詐騙類型資訊。公眾教育工作通過物理和數位平臺以及主流和社交媒體平臺進行。這包括頻繁向媒體發佈新聞稿、在“犯罪觀察”節目中進行特寫、在HDB電梯大堂的數字顯示屏上播放簡短視頻，以及定期發佈詐騙簡報和專欄。例如，自2023年11月以來，SPF一直在與新加坡報業控股合作，在本地報紙的四種語言中每月兩次發表詐騙專欄。

(五)動員組織和社區共同對抗詐騙：SPF動員社區合作夥伴在打擊詐騙方面發揮更積極的作用。在2023年，又舉行了兩次保護社區免受詐騙的可行措施對話會（C-SCAMS），針對青年和移民工人。通過這些會議，參與者討論了如何更好地保護不同人群免受詐騙，以及組織如何與政府合作，更有效地向不同人群進行外展。2023年通過C-SCAMS系列活動，與超過110名參與者和30個組織進行了互動。

(六)電子商務市場交易安全評級（“TSR”）：電子商務市場TSR於2022年5月推出，旨在教育消費者瞭解不同電子商務市場擁有的安全特性，以保護他們免受詐騙。2023年，Facebook Marketplace繼續被評為最差（一勾），因為該平臺未實施推薦的安全措施，例如針對政府頒發的記錄進行使用者驗證，並且經歷了大量的電子商務詐騙報告（2022年有1,138起案件，占總詐騙案件的23.9%）。已實施推薦的用戶驗證措施的平臺（即亞馬遜、Lazada、Qoo10）詐騙報告數量較少，因此獲得了滿分四勾的TSR評級。

肆、臺星共打合作機制

以臺星警方跨國合作為例，基於地緣關係，雙邊往來維持良好的互動關係。我國自2019

年2月1日開始設立駐星警察聯絡官後，雙方合作更趨頻繁。自2021年3月間，透過聯絡官居間協調安排，促成台星兩國警方建立共同打擊跨境詐騙犯罪境外取證合作機制，洽由我國刑事警察局提供星方運用科技辦案IP反查技術，指派專人(聯絡官)與星警商業事務局反詐騙指揮部成立專案小組，側錄被害人與詐騙歹徒對話溯源反查詐騙機房IP，委請星警製作筆錄，提供台灣檢警運用立案偵查跨境詐騙犯罪。我方得以參與當時星方反詐騙指揮部採行FRONTIER「追回款項行動網絡小組之激效對策」(Funds Recovery Operations & Networks Team, Inspiring Effective Resolutions)發揮其功能令警方與相關銀行賬戶可以迅速凍結被害人詐騙匯款。

台星合作在境外取證及共同偵辦跨國刑案部分，針對詐騙案被害人筆錄製作及情資交換案件，並成功攔截返還詐騙被害人財損等成效如下：

一、透過專案合作機制，成功協助國內檢警緊急攔截止付：2021 年共 2 件 35 萬 8,846 美元。2022 年凍結多筆受害匯入星國帳戶逾 200 萬美元。

二、臺星合作 IP 反查作業：針對境外被害人與詐騙集團成員對話機會，進行攔截通訊封包作業，採取迅速且有效的溯源任務，取得可靠 IP 位址而掌握位處國內之詐騙機房，同時製作筆錄取證完整，交付國內檢警立案，統計自 2021 年 3 月迄今立案逾 80 件。

三、因 IP 反查而偵破案件：2021 年共偵破 4 件新加坡 COIS 詐騙集團；2022 年偵破 2 件 COIS 詐騙集團，共逮捕 64 人。

四、經由持續深化及建立與星方全面性之跨國共辦合作關係，終能克服跨國取證困難之處，獲得我國駐新加坡代表處支持以官方管道提供國內有關臺星詐騙案被害人書證資料令檢察官據以起訴及法官判刑確定。

(相關照片將於簡報顯示)

伍、結論與建議

新加坡政府與多個利害關係者(Stakeholders)合作，通過與行業和國際合作夥伴的夥伴關係，在整個政府範圍內打擊詐騙。反詐騙指揮部與100多個利害關係者合作打擊詐騙更於2023年查獲近20,000個銀行帳戶，追回超過1億星幣，與外國執法夥伴合作，從海外行動中搗毀了19個針對新加坡受害者的詐騙集團。由此可以看出詐騙星國的集團與機房幾乎全部設在境外，星國警方或將參考台灣增額選派聯絡官赴外國實地合作打擊詐騙的模式，有效遏止詐騙橫行。

星國政府透過加強立法槓桿，以應對網路危害和洗錢防制問題，與銀行合作，為銀行應用程式引入反惡意軟體安全功能。以上強化識詐教育以警惕的公眾以保護新加坡免受詐騙等作為，將可做為我國識詐防詐工作重要參考，而星國所制定新頒的網路犯罪危害法甫於今年生效施行，其懲詐效果頗值得深入追蹤以觀察其後續的實益成效。(註：至於重懲重罰遏阻效果，則對境外案犯恐難生效，畢竟查緝境外涉詐嫌犯深具難度，且將遇諸多現實因素，無法順利將人犯引渡回新加坡受審…)

本文希望藉由介紹新加坡等各國關於詐騙立法例及打詐政策實踐，增進彼此交流與理解，增進我國與新加坡等各國執法機關之間國際執法合作關係，在互信互助基礎上，以更具效率的模式共同打擊跨境詐欺犯罪。

引言人2：中央警察大學行政警察學系 許福生主任

〈主題：日本打詐模式〉

日本打詐策略

許福生
中央警察大學行政警察學系教授兼系主任

令和３年版犯罪白書

令和３年版犯罪白書表紙画像
—詐欺事犯者の実態と処遇—

日本特殊詐騙之定義

- 係指不與被害者面對面，而是以電話或是電子郵件等非接觸方式，向不特定多數人騙取金錢的犯罪類型，雖然此種行為多成立詐欺罪，但視其具體實行的手法，也可能成立竊盜罪或是恐嚇取財罪等。

日本特殊詐騙之特徵

- 以集團性方式實行之，每個人均有其角色分擔
- 如打電話對被害人進行詐騙者（架け子）
- 前去受領現金的受領者（受け子）
- 把被害人匯入人頭帳戶提領金錢者（出し子）
- 明知會被用於犯罪，還是提供人頭帳戶、人頭電話，犯罪地點者（道具屋）
- 集團成員會不斷變更，也會彼此分享情報，故也有對應社會情勢的變化，靈活的改變其犯罪手段的能力

資料來源：天下雜誌787期—白領詐騙

日本特殊詐騙之類型

犯罪類型	犯罪手法
①「是我啊」詐騙 （オレオレ詐欺）	扮成親人、警察、律師，以對於親人所招致的事故的和解金為目的騙取或脅迫取得金錢。
②存款詐騙 （預貯金詐欺）	扮成親人、警察、銀行職員等，以被害人的帳戶被犯罪所利用，故需要進行更換提款卡手續等為名目，騙取或脅迫取得提款卡、信用卡、存摺。
③請求支付虛構費用詐騙 （架空料金請求詐欺）	捏造有費用未繳等事實為理由，騙取或脅迫取得金錢。

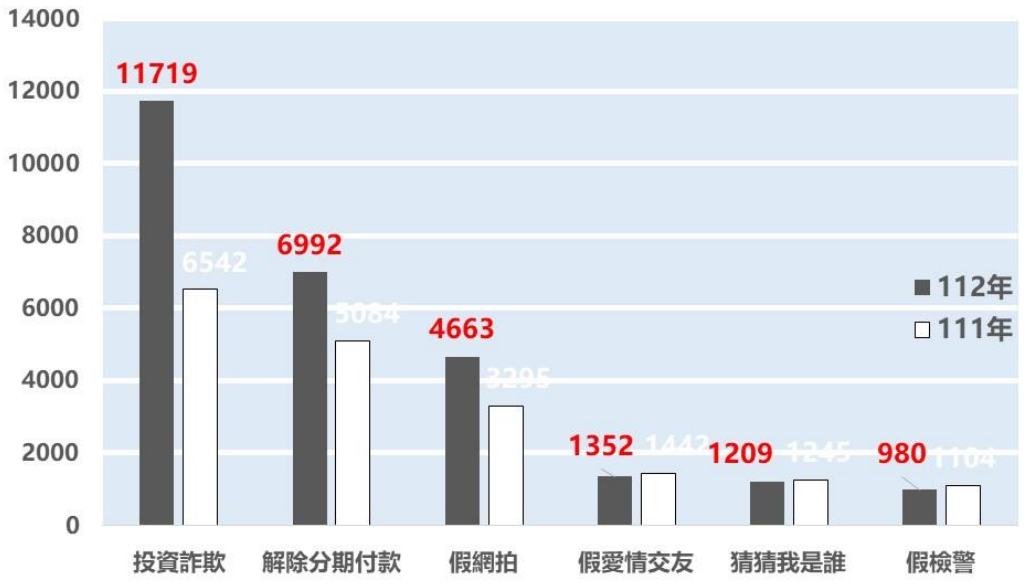
資料來源：洪兆承，日本特殊詐騙犯罪的發展與防治策略之法制簡介，當代法律，2022.08

日本特殊詐騙之類型

④退還金詐騙 （還付金詐欺）	以進行必要的手續退還稅金等為口實，讓被害者操作 ATM，以帳戶匯款的方式得到財產上的不法利益的一般詐欺事件或電子計算機詐欺事件等。
⑤金融商品詐騙 （金融商品詐欺）	提供關於虛構或是缺乏價值的未公開股、社債等有價證券、外國貨幣、高價物品等虛偽的情報，使被害者誤信購入可以獲得莫大的利益，以購入商品為由，騙取或威脅取得金錢的類型。也包含對於上述金融商品，讓無購入意思的被害人借出名義後，以解決借出名義導致的麻煩事為由，騙取或威脅取得金錢的案例。
⑥賭博詐騙 （ギャンブル詐欺）	在不特定多數人購入的雜誌中刊載「徵求打小鋼珠的人」等廣告，或是對不特定多數人寄送同樣內容的電子郵件後，對於回應上述廣告申請登錄會員的被害者，以入會費或情報費為藉口，騙取或威脅取得金錢的案例。
⑦交際斡旋詐騙 （交際あっせん詐欺）	在不特定多數人購入的雜誌中刊載「介紹異性」等廣告，或是對不特定多數人寄送「介紹異性」等內容的電子郵件後，對於回應上述廣告要求介紹異性的被害者，以入會費或情報費為藉口，騙取或威脅取得金錢的案例。
⑧提款卡詐欺竊盜 キャッシュカード詐欺盜	偽裝成警察、銀行職員或百貨公司的職員打電話給被害者，以「提款卡被他人不當利用」為由，使其準備提款卡，然後趁隙竊取的案例。
⑨其他的特殊詐欺	上述案例以外的特殊詐欺

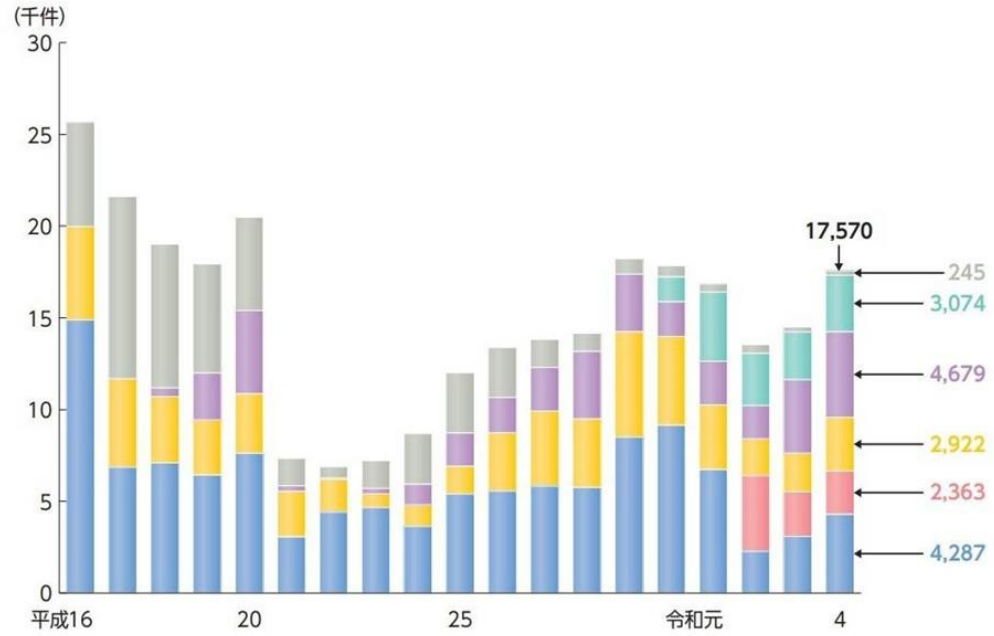
臺灣詐欺犯罪手法

（資料來源：警政署刑案紀錄表）



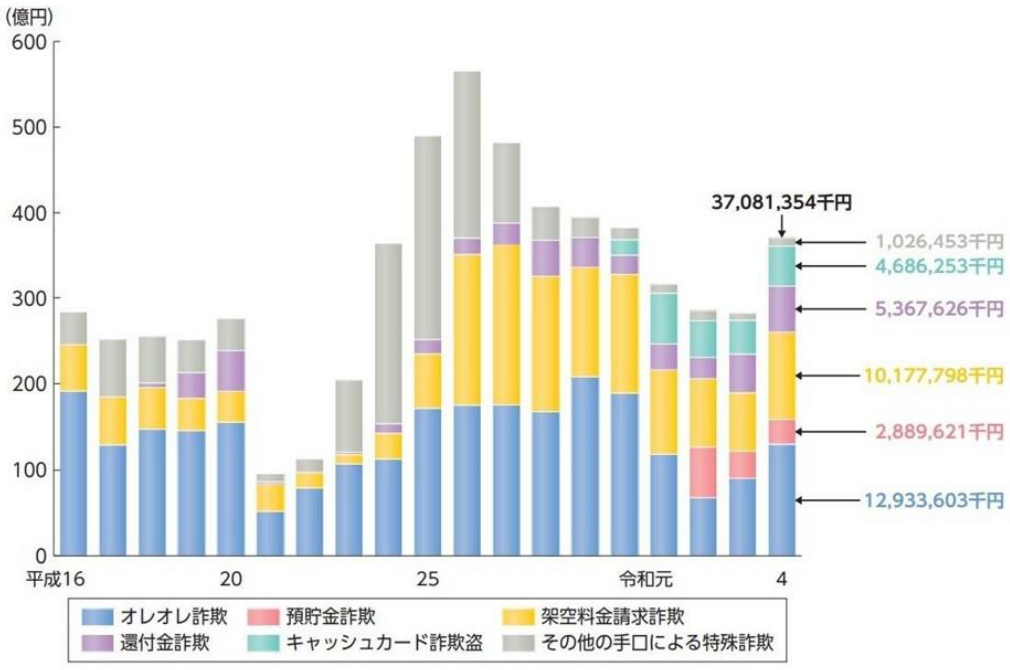
日本詐欺發生件數

① 認知件数



日本詐欺犯罪財損

③ 被害総額



臺灣詐欺犯罪趨勢

（資料來源：警政署刑案紀錄表）

日本的防治策略

2008 年提出「撲滅匯款詐騙（振り込め詐欺）行動計畫」

- 1.徹底檢舉匯款詐欺
- 2.徹底實行於 ATM 周邊的相關對策
- 3.掃蕩匿名的手機與帳戶
- 4.徹底進行被害預防的相關宣傳活動
- 5.法制面與執行面上提出諸多措施，期能打造能夠有效取締，難以讓人輕易的實行犯行的環境

日本警視廳當時將最常發生的四種詐欺型態（即「是我啊」、存款、請求支付虛構費用、退還金）統稱為「匯款詐欺」

日本的防治策略

2019 年時召開犯罪對策閣僚會議，提出「『是我啊』詐騙對策計畫」（オレオレ詐欺等対策プラン）

- 1.防止被害
- 2.管制犯行工具
- 3.有效取締犯罪

日本重要防制詐欺法制

一、行動電話不正利用防止法

- 日本於2005年公告「行動電話不正利用防止法」，並於2008年修法時將特定契約者記錄媒體（SIM卡）納入定義規制（所謂特定契約者記錄媒體係指記錄為特定與行動通話業者）。
- 賦予通訊業者在販賣或是出租手機、sim 卡等通訊設備與紀錄媒體、或是當使用者讓渡其相關通訊設備與紀錄媒體給他人時，都有確認該使用人身分，作成並保管確認紀錄的義務，通訊業者亦可在其監督下，讓媒介通訊業者履行上述義務；購買者、承租者、受讓者亦有配合提供提供駕照等證明其為本人資料的義務。
- 違反者科予刑責

日本重要防制詐欺法制

二、犯罪收益移轉防止法

- 為了防止人頭帳戶被不當利用，於2004 年制定金融機關本人確認法，對於讓渡帳戶、取得帳戶以及勸誘讓渡帳戶行為均規定了罰則。
- 2007年制定了犯罪收益移轉防止法，導致金融機關本人確認法在同年廢止，但相關規定已納入犯罪收益防止法第28條以下並經多次修正。
- 根據現行條文規定，以偽裝成他人利用存款帳戶，從金融機關受領帳戶內的存款或讓第三人受領為目的，而取得存摺或是提款卡等與匯款有關的情報之人，處以1年以下有期懲役或 100 萬以下之罰金。
- 除帳戶提款以外，對於匯兌交易與加密貨幣交易亦設有類似之規定。

日本重要防制詐欺法制

三、匯款詐騙救濟法

- 當被害人發現遭到詐騙之後，如何迅速追回財產，並補償被害人也是重要的課題。對此日本除了有針對組織犯罪處罰法相關犯罪的被害回復給付金支給制度外，於2007 年也制定了匯款詐騙濟法於2008年實行。
- 該法具體規定了以下方式，以迅速回復詐騙被害人所遭受的財產損失：

  1.凍結帳戶等措施

  2.債權消滅程序

  3.支付分配金

日本特殊詐騙防治之成效與困境

- 從數據看2009呈現大幅下降趨勢 ，但近年又有增加趨勢，2022 年（令和4年)發生數為17,570件財損、370億日圓，但未像先前超過2萬件。
- 惟鑑於特殊詐騙具有匿名性、組織性、手法多元性、廣域性、跨境性等特性，具體防治確實有其困難性。
- 如對匯款方式從要求被害人匯款至人頭帳戶改以如直接取得被詐騙的金錢（取得現金型），或是利用宅配等方式（配送現金型）來取得金錢 。
- 偵查實務採取面交逮捕方式(だまされたふり作戦)，但仍會面臨刑事法上犯意證明問題。

日本特殊詐騙防治之成效與困境

- 「行動電話不正利用防止法」 實施後，2015年至2019年間，對6萬件行動電話進行解約。
- 2016年到2019年之間，提供被犯罪所利用之行動電話的租賃公司，由240家減到了20家，可見本法有發揮一定程度效果。
- 逃避規制的方法:以MVNO為中心(相當於第二類電信服務業者)
- 使用不受規制的方法:以固定電話號碼為中心，只能一定期間內停止服務，而不能直接解約。
- 仍需進一步思考對策，特別是日本八成以上被害人是65歲以上高齡者，使用室內電話頗多。

打詐五法
立院三讀通過進度

法案	修正內容	進度
個人資料保護法	1.非公務機關保有個資外洩，最重罰1500萬 2.設立個人資料保護委員會	5月16日 三讀通過
刑法	1.3人以上同對被害人剝奪行動自由或凌虐被害人 2.以電腦合或或其他科技詐欺 以上皆罰最重7年有期徒刑，併科100萬罰金	5月16日 三讀通過
人口販運防制法	1.犯者把人騙到機場，犯行未遂，最重7年有期徒刑 2.恐嚇、拘禁等迫使人工作，最重5年有期徒刑，併科300萬罰金	5月19日 三讀通過
洗錢防制法	無正常理由收集帳戶、向虛擬平台或第三方支付申請帳戶，最重5年、拘役或併科3千萬罰金	5月19日 三讀通過
證券投資信託及顧問法	1.網路投資廣告實名制 2.刊登有價證券及業務招攬的六大禁令 3.網路平台五大義務，違反刊登者將負連帶賠償	5月3日初審 尚未三讀

ETtoday新聞雲

投顧法於5月30日三讀通過

問題與局限(113.02.19聯合報)

下架近5萬則 假投資廣告不斷

【記者李奕昕／台北報導】政府部門積極打詐，針對詐騙集團在網路平台投放假投資詐騙廣告，假冒財經、政商等公眾人物招募投資，刑事局半年通知網路平台下架近五萬則涉及假投資廣告，卻發現通知下架廣告內容仍持續出現，呼籲平台業者應負起社會責任，落實源頭管理。

證券投資信託及顧問法修正，處罰經警方通知涉假投資廣告卻未下架的網路平台，去年六月卅日施行。刑事局每日蒐報，彙整金管會證券期貨局提供資料，去年六月卅日至十二月卅一日共通知網路平台下架四萬九八一九則廣告。

刑事局統計通知下架廣告，臉書四萬六九四一件、YouTube一三二四件、Google聯播網五五四件；被冒名人士類別，財經名人占百分之八十一點五一最多，其餘依序為企業領袖百分之九點四、媒體網紅百分之五點六、政治人物百分之二點四八。

刑事局說，經查發現曾通報下架相同內容廣告仍持續出現，顯見網路平台業者未落實源頭管理；遏止違法廣告不能單憑警方通報下架，需業者擔負企業社會責任配合，發現違法主動移除、限制瀏覽等；刑事局將定期公告假投資廣告蒐報件數及話術，協助民眾辨識。

刑事局提醒，投資應透過合法管道，辨識名人廣告有無官方認證，勿輕信網路廣告、網友推薦獲利率顯不合理的投資管道，標榜加入投資老師ＬＩＮＥ群組、私訊獲飆股資訊等廣告，一定是詐騙，民眾有疑問可撥打一六五反詐騙專線諮詢。

- ◉ 只處理詐騙廣告，不處理詐騙帳號
- ◉ 只要求下架不要求平台要避免類似資訊重複上架

	台灣	日本
分工架構	菜商、機房、水房、車商	架け子、受け子、出し子、道具屋
類型	投資詐欺、解決分期付款、假網拍、假愛情交友、猜猜我是誰	「是我啊」、存款、請求支付虛構費用、退還金、金融商品、賭博、交際斡旋、提款卡詐欺竊盜、其他等詐騙
發生件數	2023年37,984件	2022年17,570件
財損	2023年88.87億元	2022年370億日幣(約77.77億元)
策略	新世代打擊詐欺策略行動綱領1.5版 1.識詐（教育宣導面） 2.堵詐（電信網路面） 3.阻詐（贓款流向面) 4.懲詐（偵查打擊面）	2008 年「撲滅匯款詐騙（振り込め詐欺）行動計畫」 1.徹底檢舉匯款詐欺 2.徹底實行 ATM 周邊相關對策 3.掃蕩匿名的手機與帳戶 4.徹底進行被害預防的相關宣傳活動 5.法制面與執行面上提出諸多措施，打造能有效取締，難以讓人輕易實行犯行的環境

	台灣	日本
被害年齡性別	假投資平均年齡為43.3歲，女性占53.51%	七成是65歲以上高齡者被害，女性為男性的1.3倍
重要法制	打詐五法 刑法、人口販運防制法、個人資料保護法、洗錢防制法、證券投資信託及顧問法	1.行動電話不正利用防止法 2.犯罪收益移轉防止法 3.匯款詐騙救濟法 4.關於透過犯罪被害財產等支付被害回復補償金法律
困境	下架近五萬假投資廣告不斷	以MVNO為中心 以固定電話號碼為中心
心得	1.詐騙具匿名性、組織性、手法多元性、廣域性、跨境性等特性防治確有其困難性 2.詐騙手法圍繞著人們「慾望」和「恐懼」像傳染病毒不斷變化 3.詐騙犯罪成為信任與價值之戰 4.要讓被害人說出來，阻止更多人受騙確實重要 5.公私協力一起來合力打擊詐騙犯罪，以遏制詐騙歪風 6.減災重於查處，目前更需要的是預防性及授權科技偵查法令	

一、如何讓被害人願意說出來阻止更多人受騙

- 當被害人發現遭到詐騙之後，如何迅速追回財產，並補償被害人，是被害人最關心的課題。日本法制上設計了國家將犯罪人從被害人那兒獲得的財產予以沒收、追徵後，用於回復被害人所蒙受的損害，設計了被害回復補償金制度，可供我國未來立法參考。
- 依據「關於透過犯罪被害財產等支付被害回復補償金法律」(犯罪被害財産等による被害回復給付金の支給に関する法律)（2006年法律第87号）規定，對於沒收、追徵的犯罪財產，作為被害回復補償金支付給被害人。

一、如何讓被害人願意說出來阻止更多人受騙

- 依據「關於從犯罪用存款帳戶等相關資金支付被害回復分配金法律」(犯罪利用預金口座等に係る資金による被害回復分配金の支払等に関する法律)（2007年法律第133号）規定，金融機關即可將該帳戶的金錢以被害回復分配金名義，支付給匯款詐欺的被害人，被害人在申請時，也必須提出其為被害人與被害額度的資料，如果有受到其他補償與賠償，也需要提出扣除額的資料。

二、行動電話不正利用防止之規範

- 相較我國NCC於2023年推出的「電信事業受理申辦電信服務風險管理機制指引」，主要是利用行政手段進行管制；
- 日本於2005年訂定了「携帯電話不正利用防止法」，從立法、行政、司法三方並進，規定行動通話業者的確認契約對象義務、讓渡通話可能終端設備等物件時必須要盡的責任，以及賦予行政機關與業者停止提供通話服務之權限，值得我國未來立法之參考。

三、制定「電信網路詐騙防制法」

相較於日本防制法令分散於各法，我國詐騙犯罪較日本嚴重，特別是大型平台問題，有必要制定「電信網路詐騙防制法」，包括總則、電信治理、金融治理、網際網路治理、科技偵查、罰則等規定；並每年出版「打詐白皮書」檢視成效

要讓黑道又怕又痛 掃黑才能有成效

◎許福生

日前竹聯幫幫明仁會高調舉辦春酒展示經濟實力，藉以達招募幫眾行銷目的，同時經由少數媒體報導，不止混淆大眾偵查視聽，且影響政府執法威信，事後警政署也祭出一連串的掃黑措施，同時成立「掃黑專責隊」全面掃蕩黑道幫派，並結合「第三方警政」徹底溯源剷根。

現行新興黑道其違法態樣與手法已從傳統暴力討債、經營圍事娛樂業、從事都更、土地開發、光電利益、轉為涉組詐欺集團、跨境洗錢、線上賭博及販賣新興毒品，以多角化方式獲取組織金源，跨越國界，其不法利益更大、查緝更不易，且公然藉組織活動招募或吸引成員，如此掃黑的法制與策略，也需隨著黑道犯罪手法改變而調整。

「聯合國打擊跨國組織犯罪公約」，是世界上第一個針對處理跨國組織犯罪的全球性公約，其第十一條明示「應努力確保針對這些犯罪的執法措施取得最大成效，並適當考慮到震懾此種犯罪的必要性」，如此掃黑要讓黑道「怕」及「痛」才能有成效。

根據筆者多次參與黑道幫派之研究，相較於一般的服刑，「強制工作」對黑道分子更具威嚇效果，縱使釋字第八二二號解釋認「強制工作」有違憲法第八條保障人身自由意旨，但若能依憲法「比例原則」及「明顯區隔原則」再予權衡，乃是可行之制度；故立法上再次引入類似「強制技職訓練」制度，應可再思考。

由於新興黑道現行不法金流來源已轉型至電信詐欺、線上賭博等犯罪。對此情勢，運用科技偵查才能有效斷黑道金源，只是我國目前尚無科技偵查法源依據，呼應「聯合國打擊跨國組織犯罪公約」第廿條規定「並在其認為適當的情況下使用其他特殊偵查手段，如電子或其他形式的監視，以有效地打擊有組織犯罪」。如此，組織犯罪防制條例應新增使用「追蹤位置技術」及「設備端通訊監察」等規定，確實有必要。

最後，針對黑道分子高調舉辦春酒，引起社會譁然，立法上可採取「先行政後司法」手段，對於以言語、舉動、文字或其他方法，明示或暗示其為犯罪組織之成員，或與犯罪組織或其成員有關聯之行為，而在公共場所或公眾得出入之場所聚集三人以上，如舉辦春酒或告別式等類似活動機會，彰顯犯罪組織聲勢，滋擾現場秩序，令周圍民眾感到不安或恐慌，若已受該管公務員解散命令三次以上而不解散者，處以刑罰，以反制黑幫氣焰。

（作者是警察大學警察政策所教授兼所長）

評論人：銘傳大學犯罪防治學系 章光明主任

身為本會副理事長，我很高興也有責任參與本次論壇。

首先談李堅志科長有關新加坡的打詐模式介紹，李科長具有豐富國際警察合作經驗，又在警大警政研究所攻讀博士，本文無論資料內容或文章架構，皆有深度，以下是我閱讀之後發現的重點:

1. 新加坡網路詐欺問題嚴重，經政策介入，雖案件仍然增加，財損卻在減少，縣市成效；
2. 網路犯罪危害法是本文亮點，該法乃是專法策略下的立法政策；屬於綜合性立法，也就是結合行政與刑事性質；並有網絡治理的立法設計；更以行政法與行政罰積極預防詐欺犯罪；
3. 更重要的是，該法對應我國通傳會、數發部、金管會三個對應部會的責任，加以規範，賦予該等部會可採取行政管理上的強制措施；
4. 我國警察職權行使法亦可加入網路平台的場域及行為加以立法，防止危害，預防犯罪，或進一步偵查犯罪；
5. 社區警政、熱點警政、治安詐欺顧慮人口、第三方警政、預警先發式警政概念等勤務策略均實際被應用在該文的介紹中；
6. 網路跨境的特質使全球治理成為重要概念與手段，包括跨國企業的協力；

許福生主任介紹日本作為的重點如下：

1. 行動電話異樣解約，確能發揮功效；
2. 識詐、堵詐、阻詐、懲詐四種政策策略，猶如從社區到政府，進一步進入刑事司法體系的分工設計，也是具體預防詐欺犯罪的分級設計；
3. 在日本，8 成以上被害人為 65 歲以上老人，應是電話詐騙，而非網路詐騙；對比新加坡以 40-49 歲為網路詐騙被害大宗，及台灣被害者平均年齡 43 歲，似有出入；另外，女性較多詐欺被害，亦值得進一步研究；
4. 我國目前打詐五法的修法，在立法策略上屬分散立法，應可參考新加坡的專法策略，效果較佳，我國目前討論的電信網路詐騙防制法或可參考新加坡模式，而日本的詐騙財物救濟法，也可考慮置入；
5. 應賦予網路平台、系統商（新）更大責任（此即第三方警政概念）；
6. 公私協力、讓被害人說出來（被害中心、被害保護、被害者學）、減災重於查、行政手段管制不正利用行動電話、實名制等建議，都是健全社區韌性的概念；

結論：

1. 我國應訂定綜合性專法，納入通傳會(NCC)、數發部、金管會的責任，並賦予行政強制力，以預防犯罪；
2. 透過公私協力、網絡治理、全球治理，提升社區韌性，及從識詐到懲詐的復原力；
3. 各種警政策略思維均可應用在網路場域及詐騙問題；
4. 必要的人權限制是打擊詐騙所應付出的代價。

主持人結論：詮理法律事務所 陳佳瑤所長

1. 詐騙已是世界性的問題，牽涉的領域非常廣，包括金融、證券、虛擬貨幣、網路、電信…等，需要倚靠團隊合作，政府應集結相關的公務機關和民間企業通力合作、爭取時效。
2. 許福生教授提到希望在打詐專法通過之後，每年能出版一本打詐白皮書，我認為這是一個很好的構想。以前我在法務部負責反毒業務的時候也是每年皆有出版反毒報告書，顯示各界合作的成果。打詐白皮書可讓國內外人士知道我們政府在打詐方面做了哪些事、面臨哪些問題以及需要哪些合作。
3. 李堅志科長提到打詐需要國際合作，尤其是資料的傳遞(例如筆錄的訊問，要能在法院被認證為有證據能力、能被引為判決被告的資料)，我認為在打詐專法裡面需要對這方面多所著墨。