法務部司法官學院112年度委託研究案

我國網路詐欺被害調查與防制研究《成果發表》

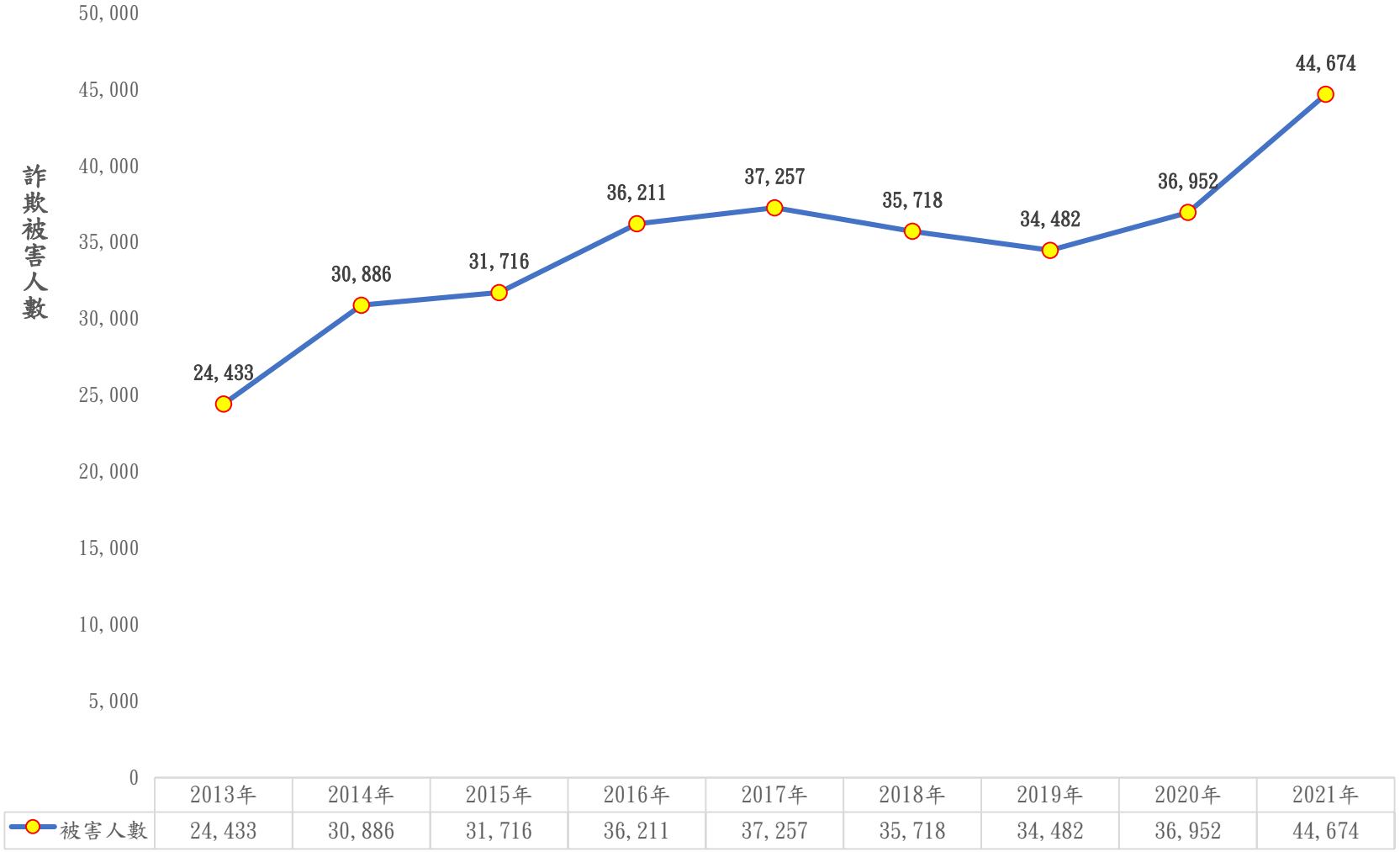
執行單位：中央警察大學
計畫主持人：賴擁連教授
協同主持人：蔡田木教授、陳玉書副教授
研究案顧問：許春金教授

研究團隊：葉碧翠助理教授、劉士誠博士生、黃百豪碩士生
研究助理：蔡文瑜博士生

網路詐欺犯罪定義

- 網路詐欺，根據刑法第 339 之 4 條第一項第三款，以廣播電視、 電子通訊、網際網路或其他媒體等傳播工具，對公眾散布而犯刑法第 339 條第一項之行為。
- 亦即行為人透過網際網路或其他媒體等傳播工具，意圖為自己或第三人不法之所有，以詐術使人將本人或第三人之物交付予行為人之行為。

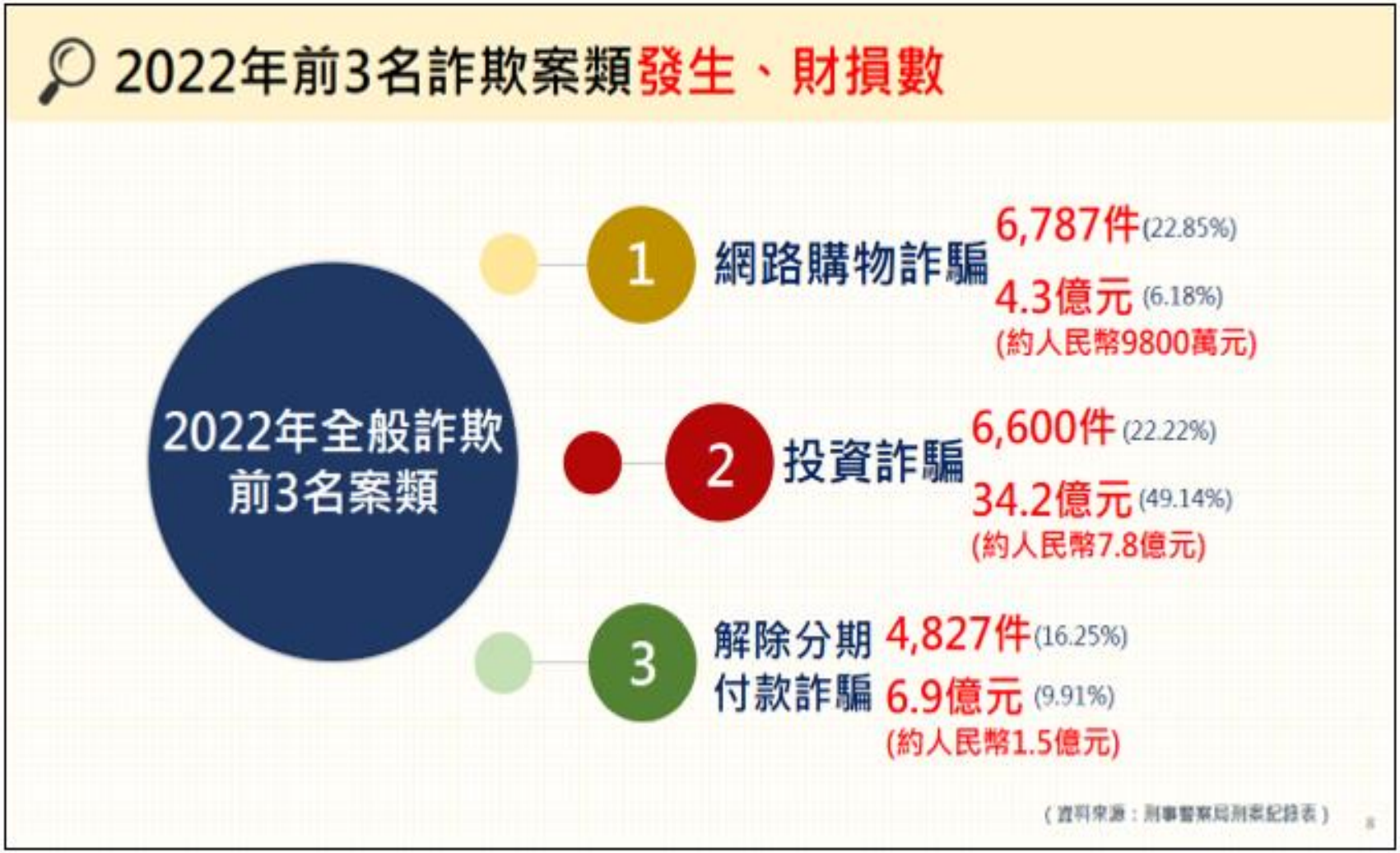
2013年至2021年詐欺被害人數統計分析



	2013年	2014年	2015年	2016年	2017年	2018年	2019年	2020年	2021年
被害人數	24,433	30,886	31,716	36,211	37,257	35,718	34,482	36,952	44,674

我國詐欺犯罪趨勢(刑事局資料)

我國前三大詐欺犯罪之類型(刑事局)



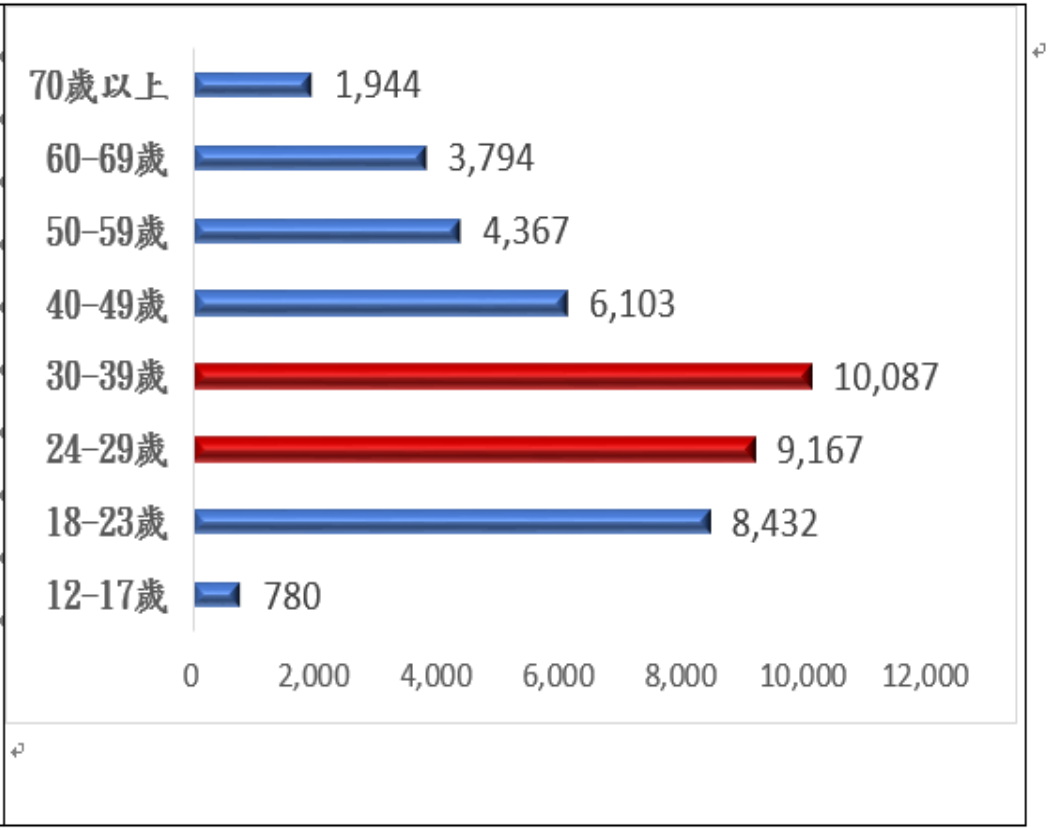
2021年詐欺被害各年齡層分布統計圖

圖 1-2

2021 年詐欺被害各年齡層分布統計圖

年齡	被害人數	%
70 歲以上	1,944	4.35
60-69 歲	3,794	8.49
50-59 歲	4,367	9.78
40-49 歲	6,103	13.66
30-39 歲	10,087	22.58
24-29 歲	9,167	20.52
18-23 歲	8,432	18.87
未滿 18 歲	780	1.75
總計	44,674	100.00

註：70 歲以上人數，包括 32 名年齡不詳之統計人數



2022年1至10月詐欺案件發生數與破獲數

犯罪方法	發生數			與上年同期比較		破獲數		與上年同期比較	
	件數	結構比(%)	當期發生數(件)	增減數(件)	增減率(%)	件數	當期發生當期破獲數(件)	增減數(件)	增減率(%)
總　計	23,927	100.00	13,965	3,622	17.84	23,398	12,878	3,311	16.48
投資詐欺	5,301	22.15	2,653	1,418	36.52	5,290	2,465	1,512	40.02
解除分期付款詐欺(ATM)	3,881	16.22	2,529	336	9.48	3,942	2,459	388	10.92
一般購物詐欺(偽稱買賣)	2,913	12.17	1,807	417	16.71	2,861	1,693	402	16.35
假網路拍賣(購物)	2,502	10.46	1,522	303	13.78	2,438	1,388	280	12.97
假愛情交友	1,184	4.95	663	229	23.98	1,137	594	179	18.68
猜猜我是誰	1,035	4.33	625	- 461	- 30.82	1,058	610	- 456	- 30.12
佯稱代辦貸款	946	3.95	611	407	75.51	925	571	423	84.26
假冒機構(公務員)	865	3.62	604	- 74	- 7.88	869	573	- 80	- 8.43
遊戲點數(含虛擬寶物)詐欺	856	3.58	526	151	21.42	829	477	130	18.60
借錢不還含票據詐欺(空頭)	819	3.42	322	37	4.73	816	304	41	5.29
假求職	709	2.96	503	292	70.02	694	473	302	77.04
盜(冒)用好友身分	443	1.85	259	- 83	- 15.78	419	237	- 112	- 21.09
其他	2,473	10.34	1,341	650	35.66	2,120	1,034	302	16.61

資料來源：警政署刑事警察局。

說明：發生數含補報發生，破獲數含破積案。

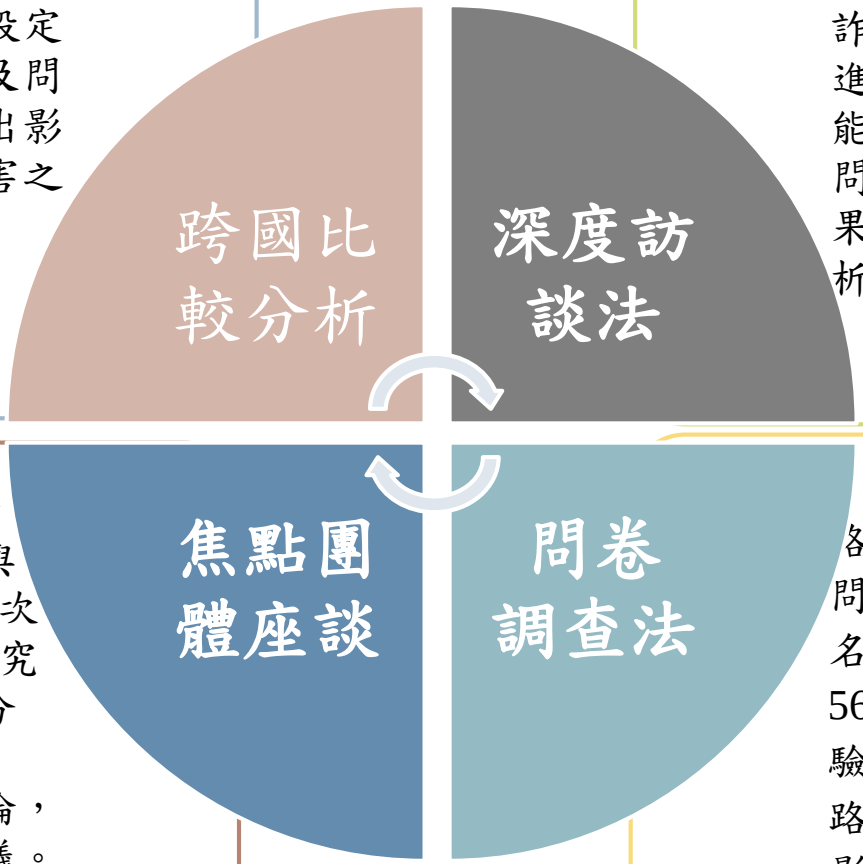
研究問題之重要性

- **深入調查網路詐欺被害經驗之必要性**：應透過網路詐欺被害經驗調查，藉以瞭解當事人的被害風險因子、被害經驗及歷程，始能掌握網路詐欺被害的真實全貌
- **詳盡探究網路詐欺被害者或被害情境之特性**：瞭解網路詐欺被害人的被害狀況、網路生活型態和情境，深入探究導致網路詐欺被害的關鍵因子
- **建立有效的網路詐欺被害預防策略與防制機制**：探究我國網路詐欺被害之現況、態樣及風險因子，並提供預防策略及防範機制之研究建議，作為刑事司法機關處理此類案件之參考，以降低犯罪被害事件之發生

研究目的

- **蒐集國、內外網路詐欺之相關調查**或官方資料中網路詐欺定義，並**編製網路詐欺被害調查問卷**，進行調查以分析網路詐欺被害者人口特性、心理特質、網路生活型態與情境機會，以及網路詐欺被害經驗等變項分布情形。
- 針對網路詐欺之定義、型態、範疇，以及網路詐欺被害調查問卷設計的妥適性，**邀請相關領域之實務、學術工作者召開專家焦點座談**，以利調查之進行。
- 於**網路問卷調查後，針對網路詐欺加害人進行質性訪談，並與網路被害調查結果進行比較分析**。
- 參考實證研究調查發現與國外防治經驗，擬訂防制對策，並邀請相關領域之實務、學術工作者**召開專家焦點座談，討論提出未來改善網路詐欺犯罪與被害之實務對策或修法建議**。
- 根據上述研究發現提出網路詐欺犯罪與被害之預防對策，並於**學術發表會發表研究成果，提供民眾與政府機關參考**。

研究設計與實施：研究方法



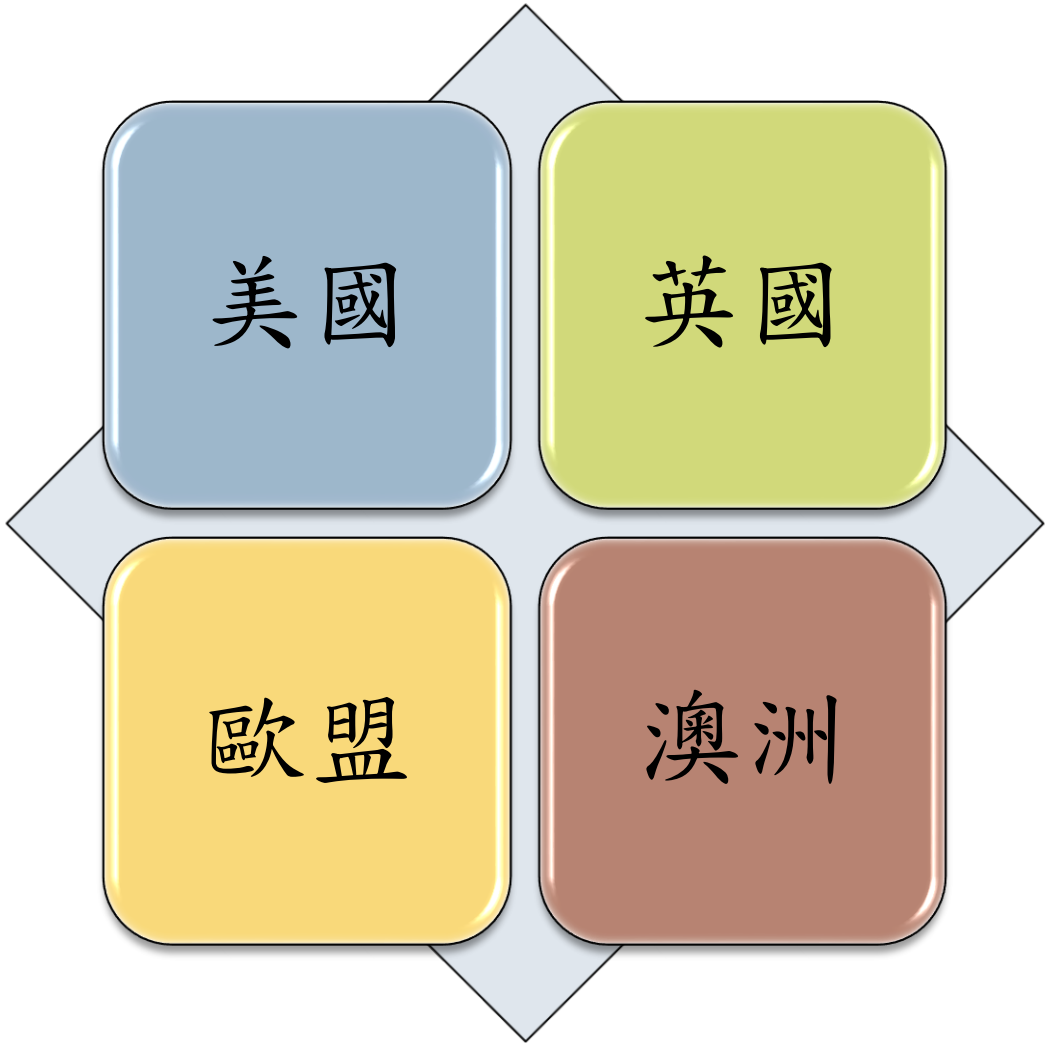
• 蒐集國內外理論與實證研究，設定網路詐欺定義及問卷題目，並找出影響網路詐欺被害之關鍵因子。

• 針對5名不同網路詐欺類型之加害人進行質性訪談。期能針對本研究網路問卷被害人調查結果之發現，進行分析與比較。

• 邀請犯罪與矯正背景之學者與專家，共計2場次9名，針對本研究問卷擬訂以及分析的初步結果，進行檢視與討論，以形塑政策建議。

• 針對1,146名網路使用者進行網路問調查，包括582名無被害經驗組及564名曾有被害經驗組。期能瞭解網路詐欺被害特性及影響因子。

跨國網路詐欺被害調查方法之比較分析

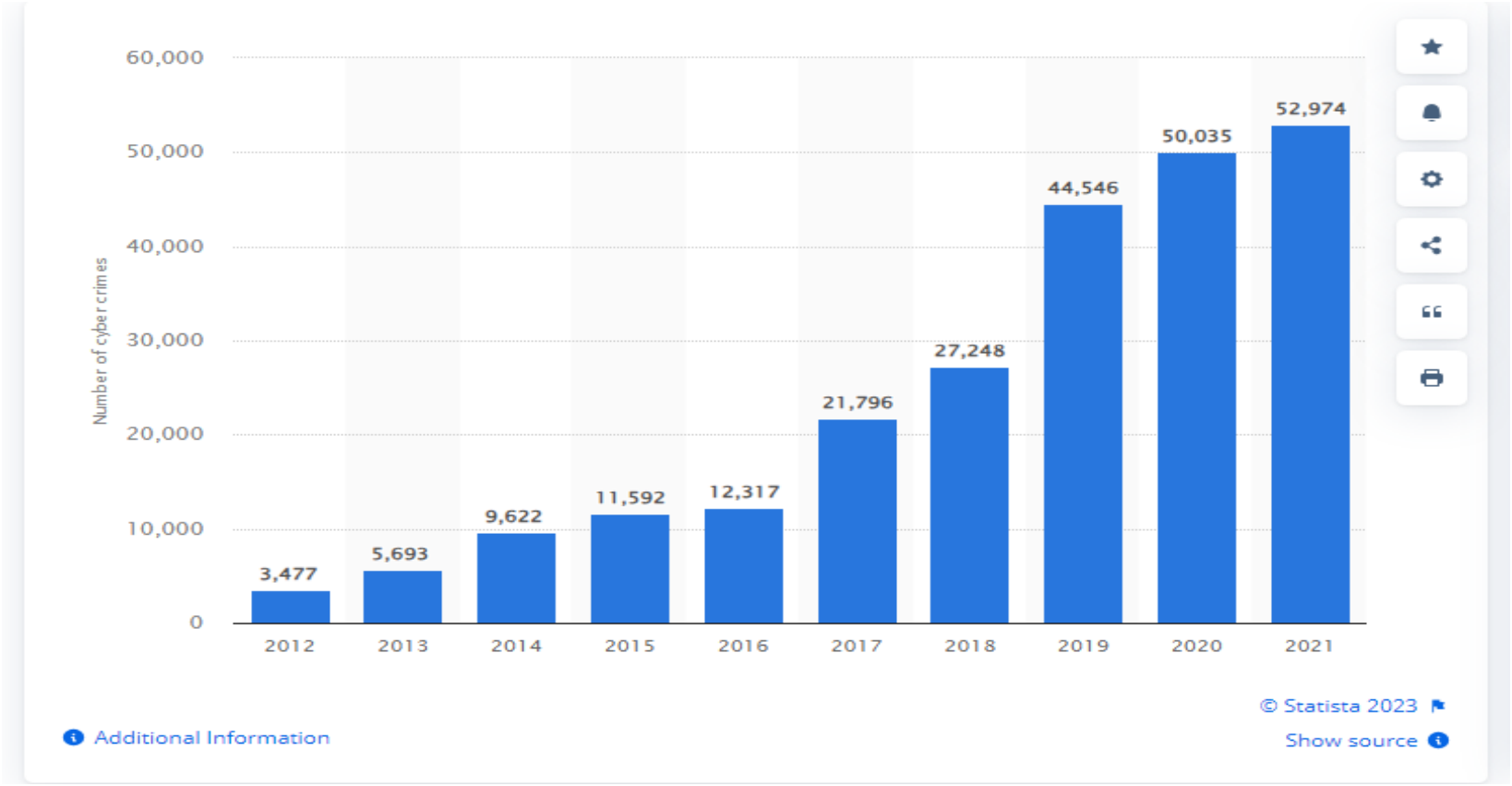


各國網路詐欺被害相關調查之情勢分析

- 網路詐欺犯罪之呈現日益嚴重之趨勢
- 網路詐欺仍以網路投資財損最為嚴重
- 各國網路詐欺之調查與報案方式已走向網路化
- 成立網路詐欺犯罪調查專責機構已成為趨勢
- 打擊網路詐欺犯罪須靠跨境/跨域合作始能克竟其功

跨國比較網路詐欺被害定義與調查之結果

- 網路詐欺犯罪之呈現日益嚴重之趨勢



示意圖, 資料來源: https://www.statista.com/statistics

網路詐欺仍以網路投資財損最為嚴重

2022 CRIME TYPES

By Victim Count

Crime Type	Victims	Crime Type	Victims
Phishing	300,497	Government Impersonation	11,554
Personal Data Breach	58,859	Advanced Fee	11,264
Non-Payment/Non-Delivery	51,679	Other	9,966
Extortion	39,416	Overpayment	6,183
Tech Support	32,538	Lottery/Sweepstakes/Inheritance	5,650
Investment	30,529	Data Breach	2,795
Identity Theft	27,922	Crimes Against Children	2,587
Credit Card/Check Fraud	22,985	Ransomware	2,385
BEC	21,832	Threats of Violence	2,224
Spoofing	20,649	IPR/Copyright/Counterfeit	2,183
Confidence/Romance	19,021	SIM Swap	2,026
Employment	14,946	Malware	762
Harassment/Stalking	11,779	Botnet	568
Real Estate	11,727		

Descriptors*			
Cryptocurrency	31,310	Cryptocurrency Wallet	20,781

*These descriptors relate to the medium or tool used to facilitate the crime and are used by the IC3 for tracking purposes only. They are available as descriptors only after another crime type has been selected. Please see Appendix B for more information regarding IC3 data.

2022 CRIME TYPES continued

By Victim Loss

Crime Type	Loss	Crime Type	Loss
Investment	$3,311,742,206	Lottery/Sweepstakes/Inheritance	$83,602,376
BEC	$2,742,354,049	SIM Swap	$72,652,571
Tech Support	$806,551,993	Extortion	$54,335,128
Personal Data Breach	$742,438,136	Employment	$52,204,269
Confidence/Romance	$735,882,192	Phishing	$52,089,159
Data Breach	$459,321,859	Overpayment	$38,335,772
Real Estate	$396,932,821	Ransomware	*$34,353,237
Non-Payment/Non-Delivery	$281,770,073	Botnet	$17,099,378
Credit Card/Check Fraud	$264,148,905	Malware	$9,326,482
Government Impersonation	$240,553,091	Harassment/Stalking	$5,621,402
Identity Theft	$189,205,793	Threats of Violence	$4,972,099
Other	$117,686,789	IPR/Copyright/Counterfeit	$4,591,177
Spoofing	$107,926,252	Crimes Against Children	$577,464
Advanced Fee	$104,325,444		

Descriptors**			
Cryptocurrency	$2,496,196,530	Cryptocurrency Wallet	$1,349,090,883

網路詐欺之調查與報案方式已走向網路化

Internet Crime Complaint Center (IC3)

File a Complaint

Prior to filing a complaint with the IC3, please read the following information regarding terms and conditions. Should you have additional questions prior to filing your complaint, view FAQs for more information on inquiries such as:

- What details will I be asked to include in my complaint?
- What happens after I file a complaint?
- How are complaints resolved?
- Should I retain evidence related to my complaint?

The information I'm providing on this form is correct to the best of my knowledge. I understand that providing false information could make me subject to fine, imprisonment, or both. (*Title 18, U.S. Code, Section 1001*)

Complaints filed via this website are processed and may be referred to federal, state, local or international law enforcement or regulatory agencies for possible investigation. I understand any investigation opened on any complaint I file on this website is initiated at the discretion of the law enforcement and/or regulatory agency receiving the complaint information.

Filing a complaint with the IC3 in no way serves as notification to my credit card company that I am disputing unauthorized charges placed on my card or that my credit card number may have been compromised. I should contact my credit card company directly to notify them of my specific concerns.

The complaint information you submit to this site is encrypted via secure socket layer (SSL) encryption. Please see the Privacy Policy for further information.

We thank you for your cooperation.

I Accept

成立網路詐欺犯罪調查專責機構已成為趨勢

- 美國自2000年成立網路犯罪報案中心(Internet Crime Complaint Center, IC3)
- 英國2016年成立國家網路安全中心(National Cyber Security Centre, NCSC)
- 澳大利亞也於2014年成立網路安全中心(Australia Cyber Security Centre, ACSC)，作為澳大利亞有關網路犯罪問題研究、調查、擬定與防制網路犯罪問題與威脅之專責機關。

打擊網路詐欺須靠跨境/跨域合作始能克竟其功

- 美國司法部與聯邦調查局(FBI)會與其他國家例如印度的中央調查局與地方執法部門合作，共同打擊金融犯罪與跨國假客服詐騙案件(FBI,2023)。
- 英國的國家網路安全中心(NCSC)在其官網宣稱該中心與美國、加拿大、澳大利亞、紐西蘭等國家級的網路安全相關部門結盟，共同打擊相關的網路犯罪、攻擊與威脅事件。

網路被害調查有效樣本分布

項目	總調查人數		完成受訪人數(不含隔離區)	
	人數	%	人數	%
符條件有效樣本	1,146	49.67	1,146	93.32
隔離區				
填答未滿 240 秒	20	0.87	20	1.63
人工檢誤刪除無效樣本	62	2.69	62	5.05
不符合調查條件樣本數	1,079	46.77	-	-
合計	2,307	100.00	1,228	100.00

註: 調查網頁總瀏覽人數為 4,365 人，含進入調查網頁開始填答而未完成調查之受訪者。

網路被害調查之研究概念與變項內容

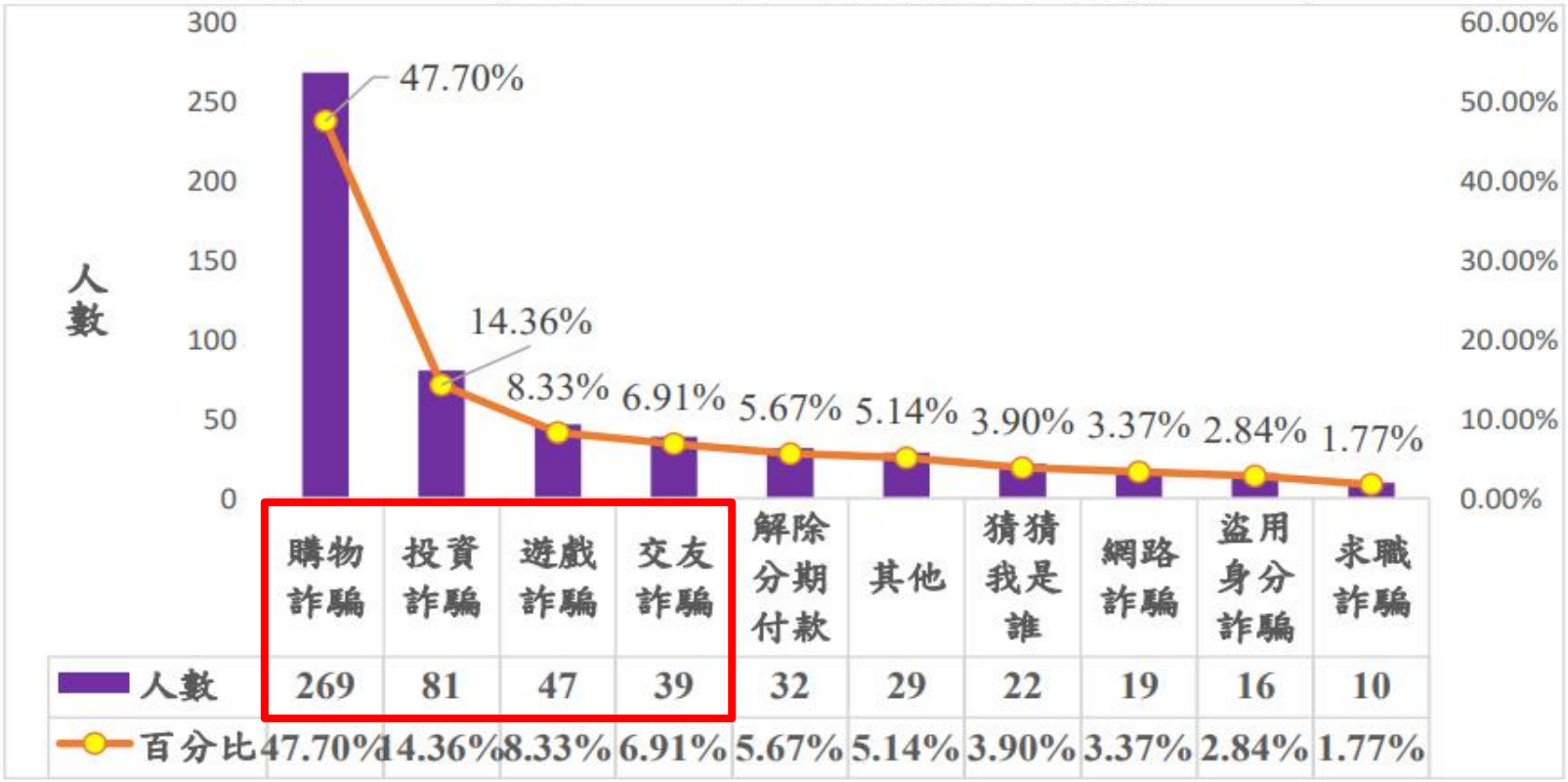
研究概念	變項內容
自變項	
人口特性	性別、年齡、職業、收入、教育程度
區域特性	區域位置、城鄉
心理特質	偏差動機、網路成癮、衝動性、冒險性、低克制能力
網路生活型態	網路使用經驗、網路風險
情境機會	防護監控、被害動機、被害誘因
依變項	
網路詐欺被害	有無被害經驗、網路詐欺被害多元性、重複被害、最近一次被害經驗

受訪者網路使用經驗測量內容

變項名稱	測量內容
每天上網時數	①1 小時以內、②1 至 2 小時以內、③2 至 4 小時以內、④4 至 6 小時以內、⑤6 小時以上，共 5 個等級。
每周上網次數	①少於 1 次、②1-3 次、③4-6 次、④7-9 次、⑤10 次以上，共 5 個等級。
周末上網時段	①08：01 至 12：00、②12：01 至 14：00、③14：01 至 18：00、④18：01 至 22：00、⑤22：01 至 02：00、⑥02：01 至 08：00，共 6 項。
接觸網路時間	①1 年未滿、②1 年～2 年未滿、③2 年～3 年未滿、④3 年～5 年未滿、⑤5 年～10 年未滿、⑥10 年以上，共 6 個等級。
擁有網路帳號	①購物網站、②線上遊戲、③網頁留言討論區、④社群軟體(TELEGRAM、LINE、IG、FB、TWITTER、WECHAT、抖音等)、⑤交友平台(TINDER、IPAIR、WETOUCH、SWEETRING、JUSTDATING、GOODNIGHT等)、⑥直播平台(抖音、BILIBILI、VOOM、西瓜視頻、土豆等)，共6類。

網路詐欺被害的犯罪類型

圖 3-3-1　最近一次網路詐欺類型分布圖(n=564)

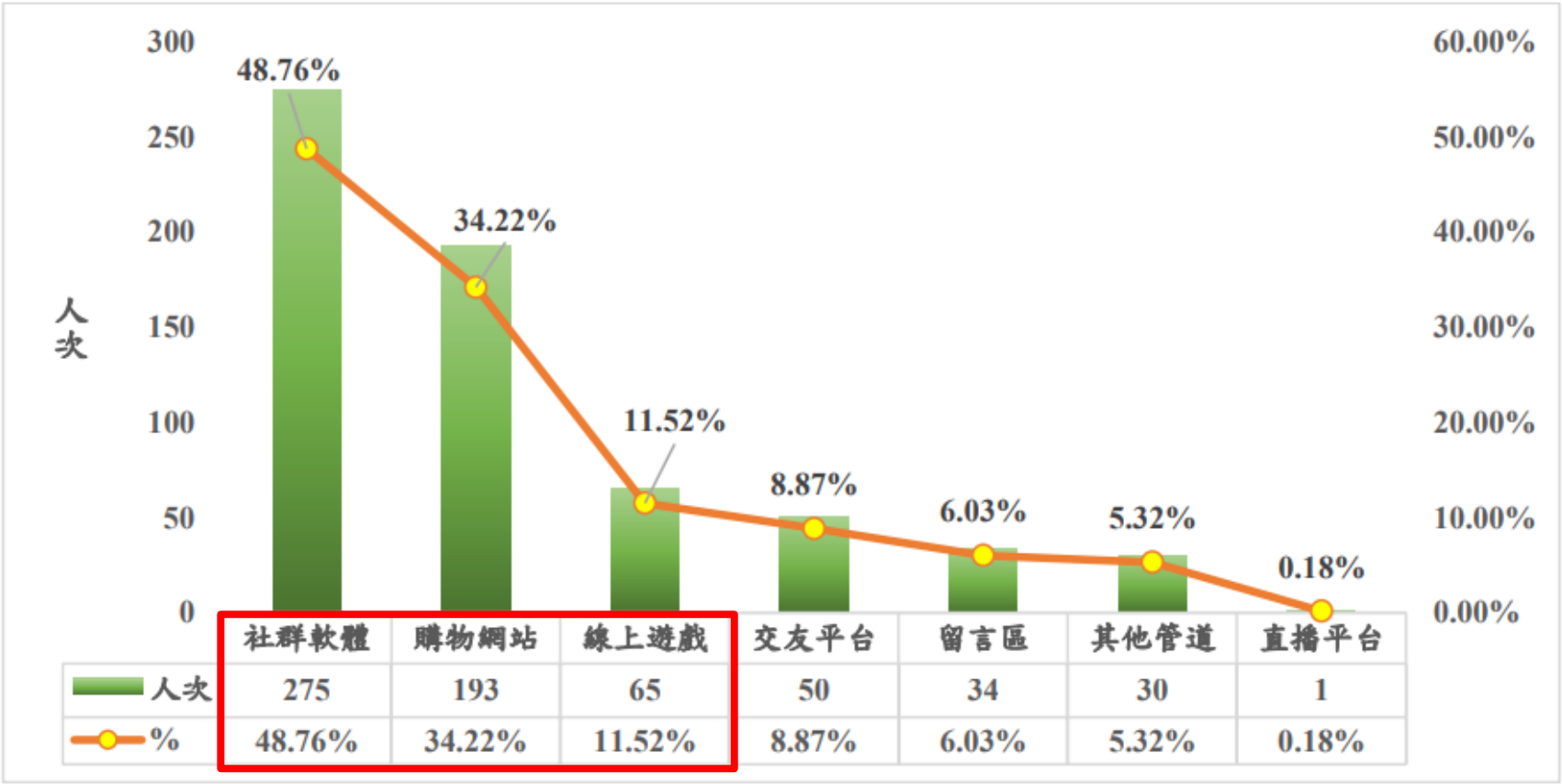


	購物詐騙	投資詐騙	遊戲詐騙	交友詐騙	解除分期付款	其他	猜猜我是誰	網路詐騙	盜用身分詐騙	求職詐騙
人數	269	81	47	39	32	29	22	19	16	10
百分比	47.70%	14.36%	8.33%	6.91%	5.67%	5.14%	3.90%	3.37%	2.84%	1.77%

註：本選項為**單選題**，其他類型詐騙，包括購買二手車、網路訂房、購買演唱會門票、簡訊詐騙等

網路使用經驗與被害管道

圖 3-3-2　最近一次網路詐欺接觸管道分布圖(n=564)

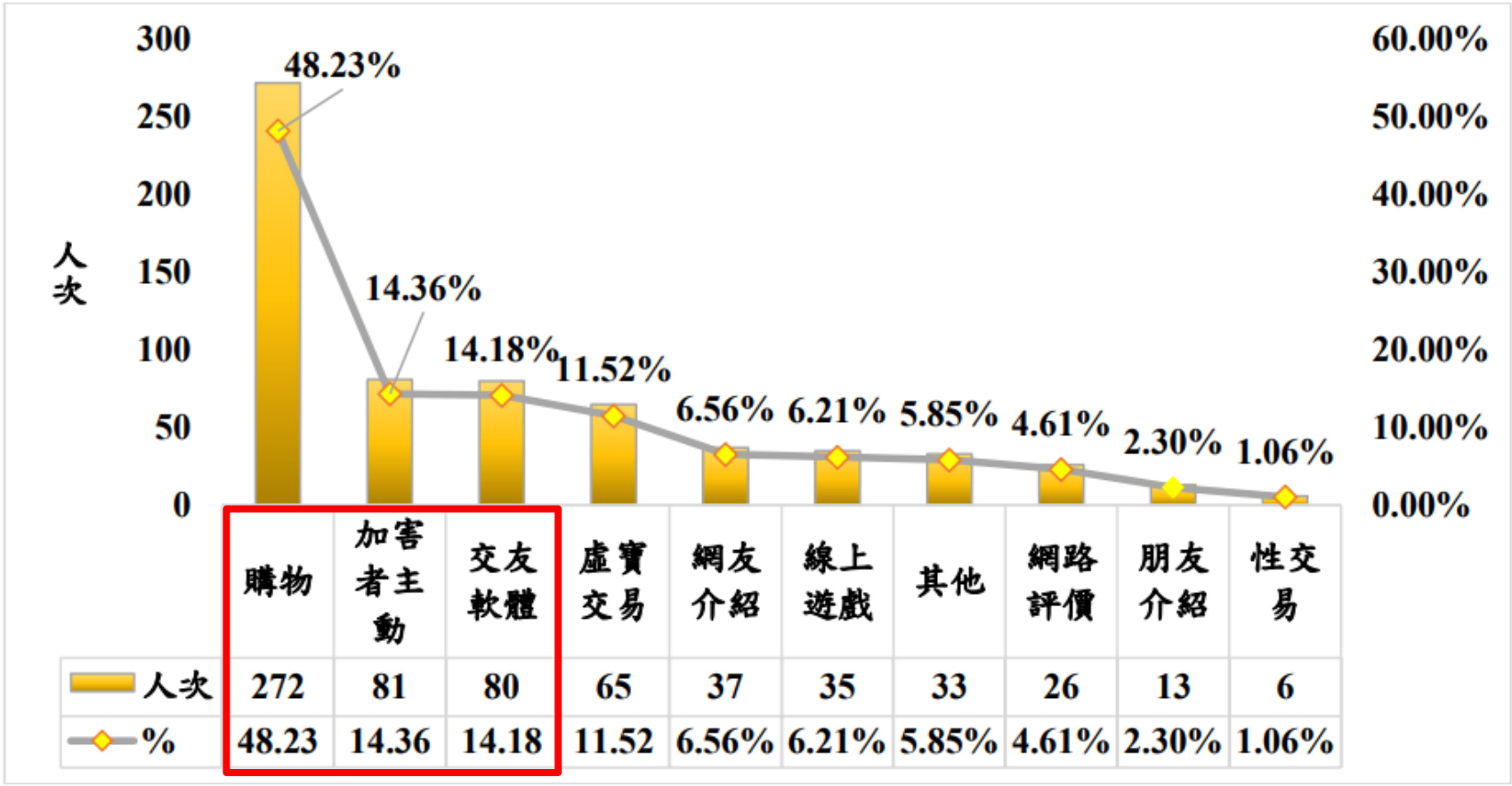


	社群軟體	購物網站	線上遊戲	交友平台	留言區	其他管道	直播平台
人次	275	193	65	50	34	30	1
%	48.76%	34.22%	11.52%	8.87%	6.03%	5.32%	0.18%

註：本選項為**複選題**，其他接觸管道，包括簡訊、電話、新聞網頁、政府機關網頁等。

網路詐欺互動情形分布

圖 3-3-3　最近一次網路詐欺互動情形分布圖(n=564)

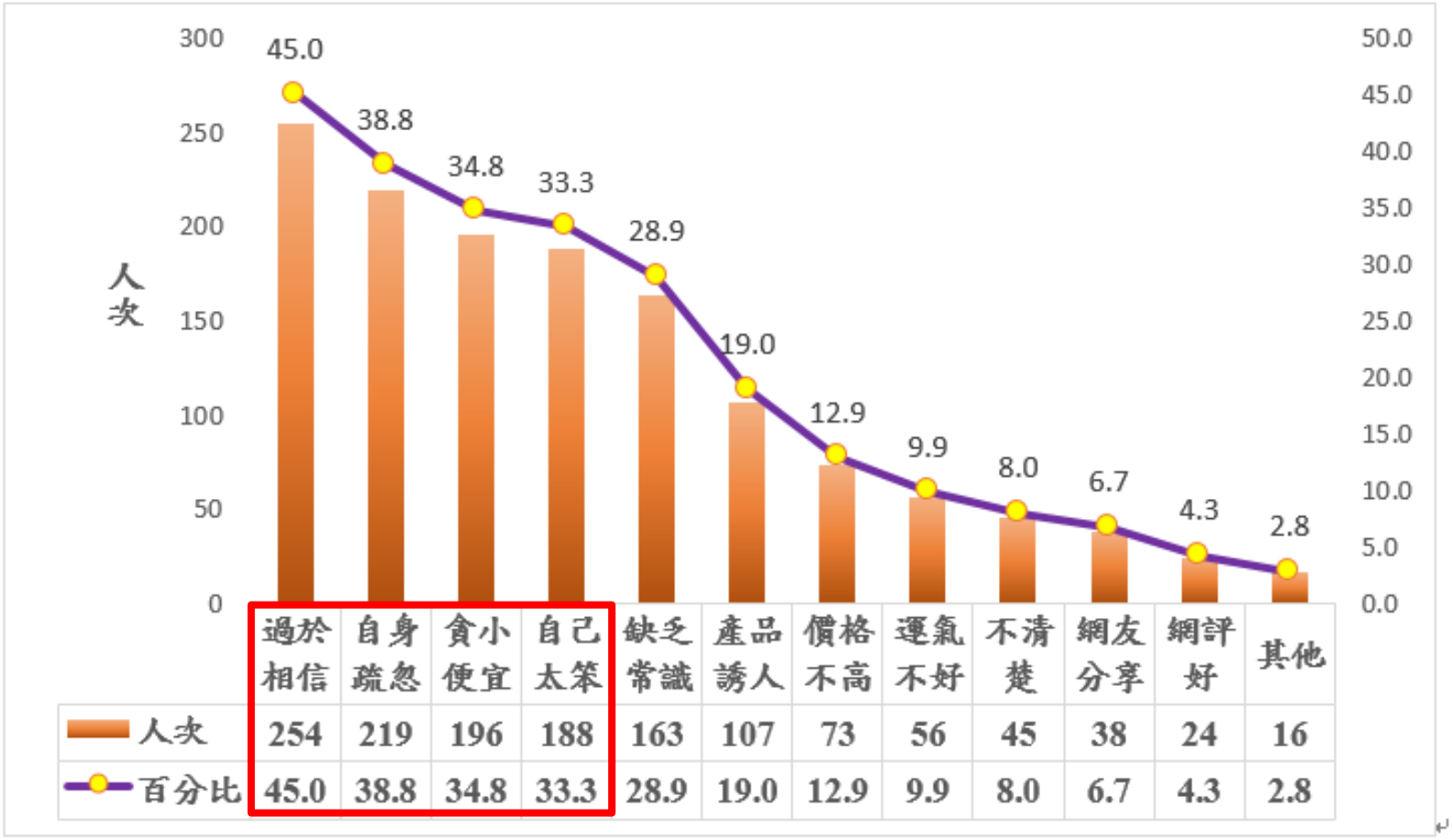


	購物	加害者主動	交友軟體	虛實交易	網友介紹	線上遊戲	其他	網路評價	朋友介紹	性交易
人次	272	81	80	65	37	35	33	26	13	6
%	48.23	14.36	14.18	11.52	6.56%	6.21%	5.85%	4.61%	2.30%	1.06%

註：本選項為**複選題**，其他接觸管道，包括寫信、簡訊、電話、介紹工作等。

網路詐欺被害原因分析

圖 3-3-4　最近一次網路詐欺被害原因分布圖(n=564)



	過於相信	自身疏忽	貪小便宜	自己太笨	缺乏常識	產品誘人	價格不高	運氣不好	不清楚	網友分享	網評好	其他
人次	254	219	196	188	163	107	73	56	45	38	24	16
百分比	45.0	38.8	34.8	33.3	28.9	19.0	12.9	9.9	8.0	6.7	4.3	2.8

最近一次網路詐欺被害經驗

表 3-3-1　網路詐欺被害事件特性分析表(n=564)

變項	人數	百分比	變項	人數	百分比
被害匯款時間(n=564)			**認識加害人程度(n=564)**		
08：01-12：00	60	10.6	熟識	14	2.5
12：01-14：00	64	11.3	普通	41	7.3
14：01-18：00	131	23.2	初識	61	10.8
18：01-22：00	**207**	**36.7**	**不認識**	**448**	**79.4**
22：01-02：00	88	15.6	**被害交易方式(n=564)**		
02：01-08：00	14	2.5	現金	42	7.4
損失金額(n=564)			超商付款	72	12.8
未滿 1 千元	**173**	**30.7**	遊戲點數	67	11.9
1,001 元至未滿 1 萬元	**178**	**31.6**	實體 ATM 轉帳	49	8.7
1 萬至未滿 3 萬元	56	9.9	信用卡	53	9.4
3 萬至未滿 10 萬元	39	6.9	**網路 ATM 轉帳付款**	**127**	**22.5**
10 萬至未滿 50 萬元	37	6.6	行動支付	15	2.7
50 萬至未滿 100 萬元	11	2.0	線上支付軟體	21	3.7
100 萬至未滿 1,000 萬元	19	3.4	金融機構匯款	42	7.4
1,000 萬元以上	3	0.5	網路銀行付款	47	8.3
沒有損失	48	8.5	其他	29	5.1

註：其他被害交易方式，包括電話騷擾、實體及網銀交易、虛擬貨幣、股票買賣等

網路詐欺被害覺察之機制與時間

表 3-3-2　網路詐欺被害察覺階段分析表(n=564)

變項	人數	百分比	變項	人數	百分比
得知被害			**警覺遭詐時間**		
自己察覺	**450**	**79.8**	**1 天以內**	**227**	**40.2**
警方通知	4	0.7	1-3 天	162	28.7
朋友或同事發現	40	7.1	4-6 天	65	11.5
親人發現	35	6.2	7-14 天	48	8.5
超商店員提醒	7	1.2	14-30 天	23	4.1
金融機構櫃檯提醒	20	3.5	30 天以上	39	6.9
其他	8	1.4			

註：本題為**單選題**，其他得知被害方式，包括擲筊、銀行通知、新聞報導、收到包裹等。

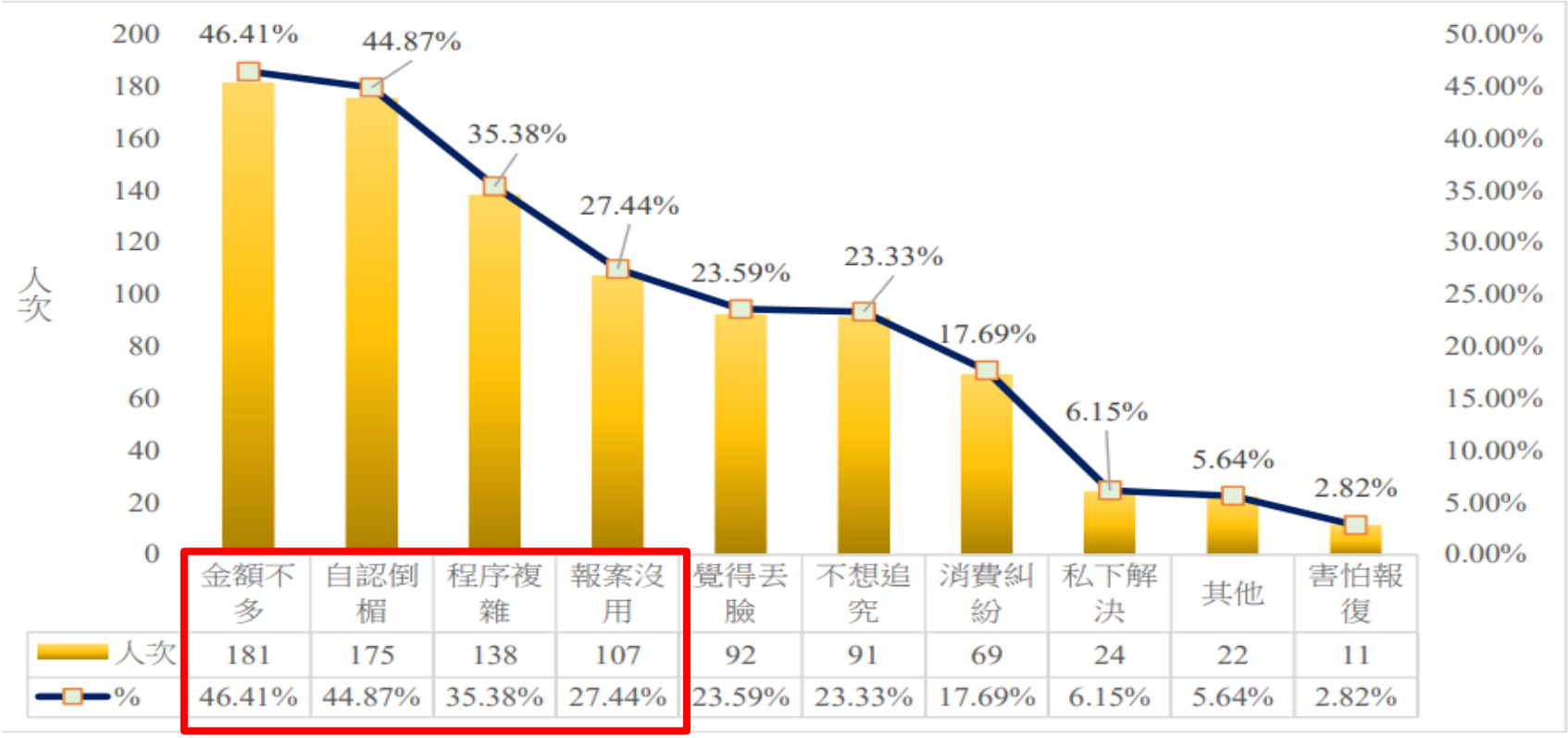
網路詐欺被害後反應情形與程度

表 3-3-3　網路詐欺被害反應階段分析表(n=564)

變項	人數	百分比	變項	人數	百分比
是否報案			**恢復正常時間**		
有	174	30.85	立即就恢復	156	27.7
無	390	69.15	**一週內**	**187**	**33.2**
焦慮程度			半個月內	69	12.2
非常嚴重	66	11.7	一個月內	46	8.2
嚴重	115	20.4	一至二個月	27	4.8
不太嚴重	**267**	**47.3**	三個月以上	40	7.1
一點也不嚴重	79	14.00	永遠難以恢復	39	6.9
沒意見/很難說	34	6	**總數**	**564**	**100**
不知道	3	0.5			

網路詐欺被害者未報案之原因分析

圖 3-3-5　最近一次網路詐欺被害未報案原因分布圖(n=390)a



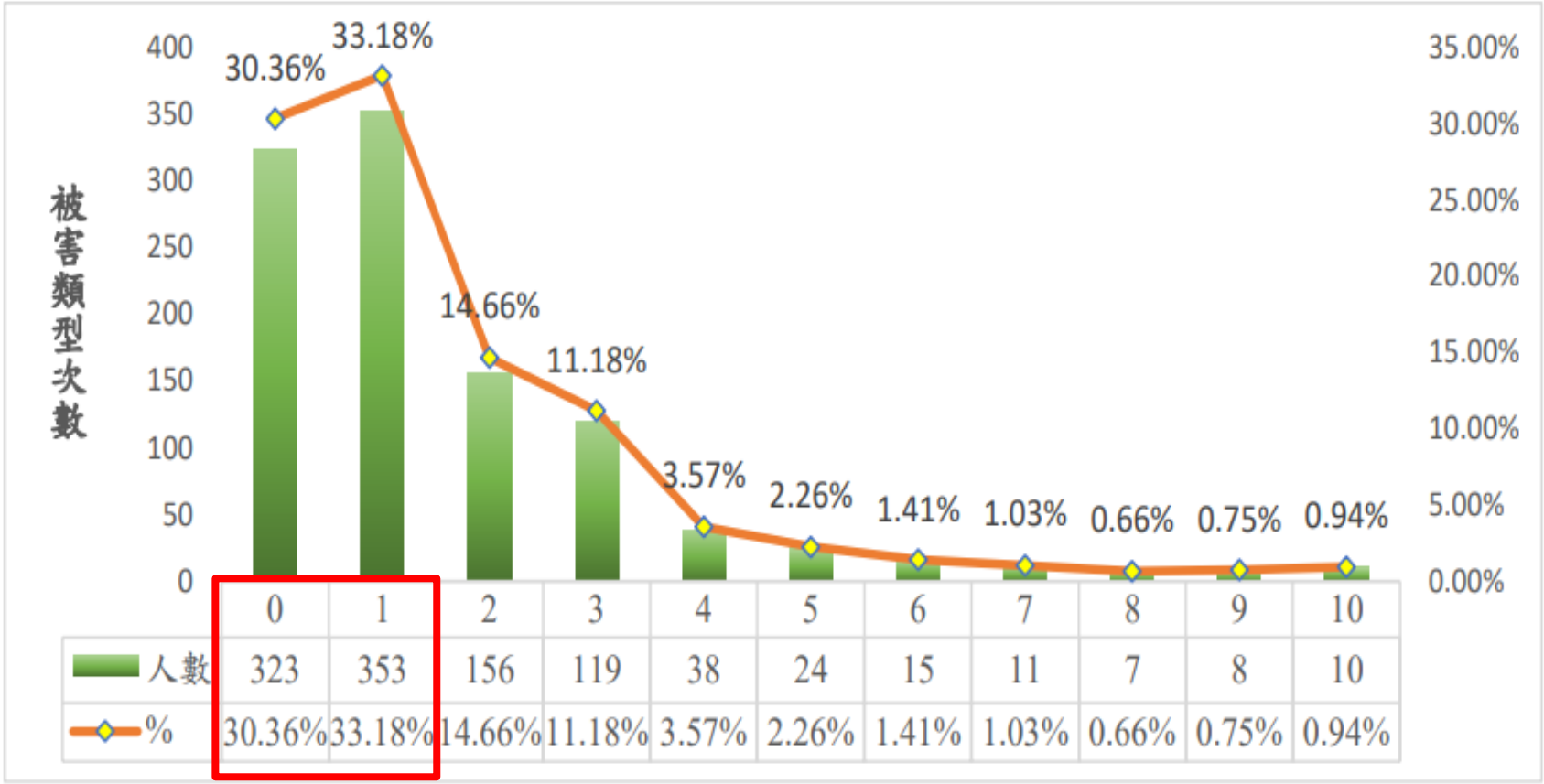
	金額不多	自認倒楣	程序複雜	報案沒用	覺得丟臉	不想追究	消費糾紛	私下解決	其他	害怕報復
人次	181	175	138	107	92	91	69	24	22	11
%	46.41%	44.87%	35.38%	27.44%	23.59%	23.33%	17.69%	6.15%	5.64%	2.82%

註：1.[a] 本研究樣本有向警方報案有 174 人(占 30.85%)，未向警方報案者 390 人(占 69.15%)，本題為探討未向警方報案之原因，故分析樣本為 390 人。

2.本題為複選題，未報案其他原因包括自身有警覺、客服處理、沒損失、政府查不到、錢有討回來等原因。

網路詐欺被害事件具有多元性與重複性

圖 3-3-8　網路詐欺被害類型之多元性分布 (n=1,064)



	0	1	2	3	4	5	6	7	8	9	10
人數	323	353	156	119	38	24	15	11	7	8	10
%	30.36%	33.18%	14.66%	11.18%	3.57%	2.26%	1.41%	1.03%	0.66%	0.75%	0.94%

註：原始樣本 1,146 名，扣除遺漏值 82 名，有效樣本為 1,064 名。

一般組與被害組之比較分析

- 人口特性(男性、40歲以下、收入介於1元以上未滿4萬元者、教育程度愈低者)與網路詐欺被害有顯著關聯性。
- 區域特性(居住地區、城鄉)則無關聯性。
- 被害組在網路使用風險、遊樂動機(瀏覽色情網站、遊玩網路遊戲與未知身分與網友聊天)與被害誘因(點擊不明來源信件、點擊不明信件附件/檔案、下載不明的檔案)顯著高於一般組
- 被害組在防護監控方面與一般組不明顯
- 被害組在偏差動機(下載非正版軟體沒關係、詐騙人家也沒關係、網路偽裝不會被發現)、網路成癮與低自我控制顯著高於一般組

網路詐欺被害的顯著影響因子

表 3-5-2　網路詐欺被害影響因素之羅吉斯迴歸分析(n=1,146)

自變項	模型一		模型二		模型三		模型四	
	B(Wald)	Exp (B)	B(Wald)	Exp (B)	B(Wald)	Exp (B)	B(Wald)	Exp (B)
人口特性								
性別 [a](1)	**0.397(10.035**)**	1.487	0.148(1.185)	1.159	0.098(0.498)	1.103	-0.159(1.085)	0.853
年齡	**-0.017(10.199**)**	0.983	**-0.015(6.611**)**	0.986	**-0.013(5.068*)**	0.987	-0.004(0.359)	0.996
收入三組 [b](1)	0.151(0.731)	1.163	0.02(0.011)	1.02	0.02(0.011)	1.02	-0.002(0)	0.998
收入三組(2)	**-0.434(4.325*)**	0.648	**-0.497(5.202*)**	0.608	**-0.528(5.743*)**	0.59	-0.418(3.4)	0.658
教育程度 [c](1)	-0.195(1.127)	0.823	-0.25(1.683)	0.779	-0.245(1.603)	0.782	-0.238(1.415)	0.788
網路成癮								
行為依賴			-0.026(1.847)	0.975	-0.029(2.213)	0.972	-0.029(2.117)	0.971
心理依賴			**0.112(22.29***)**	1.119	**0.106(19.636***)**	1.112	**0.089(12.854***)**	1.093
低自我控制								
衝動性			**0.119(13.225***)**	1.126	**0.117(12.749***)**	1.124	**0.082(5.843*)**	1.086
冒險性			0.015(0.22)	1.015	-0.005(0.021)	0.995	-0.033(0.949)	0.968
低克制力			-0.065(4.34)	0.937	-0.071(4.058)	0.931	-0.07(4.502)	0.933
偏差動機			**0.046(7.229**)**	1.047	**0.04(5.261*)**	1.041	0.014(0.571)	1.014
網路風險								
接觸偏差訊息					0.033(3.079)	1.034	-0.008(0.165)	0.992
網路觸法行為					0.088(3.551)	1.092	0.041(0.666)	1.042
防護監控								
實體監控							-0.025(0.277)	0.975
避免曝露							-0.026(0.223)	0.974
被害誘因動機								
被害誘因							**0.224(24.557***)**	1.251
被害動機							**0.173(18.768***)**	1.189
常數	0.615(5.243*)		-1.497(12.109***)		-1.935(17.066***)		-2.388(12.719***)	
-2LL 對數概似值	1548.786		1470.136		1459.232		1394.148	
H-L 檢定 (模型適配度)	χ^2=12.313; p=0.138		χ^2=8.609; p=0.376		χ^2=9.213; p=0.325		χ^2=7.041; p=0.532	
Cox & Snell R^2 (Nagelkerke R^2)	0.034 (0.045)		0.10(0.131)		0.107(0.142)		0.156(0.208)	
正確預測率	58.6		64.4		65.9		67.7	

網路詐欺加害者之受訪人數與手法

訪談對象	人數	取樣條件
觸犯刑法第 339 條詐欺罪名，且透過「網路」為犯案管道，且目前仍在監服刑之受刑人	1 人	「投資詐欺」之詐欺手法
	1 人	「電信客服人員」之詐欺手法
	3 人	「網路購物詐欺」之詐欺手法

網路詐欺加害人訪談大綱

訪談主題	訪談內容
基本資料	性別、年齡、婚姻、教育程度、初犯或再累犯等
家庭狀況	父母婚姻狀況、父母管教情形、家庭背景
學校成長經驗	國（高）中時期學習狀況、學業成績、在校適應問題、逃學與輟學經驗、
個人生活型態	就學與就業情形、交友情形與平時休閒活動、與網路詐欺犯罪之經驗等
從事網路詐欺之情形	與被害者互動情形、犯罪所得報酬、周遭監控能力、如何尋找合適的標的物、如何規避警方查緝、是否曾擔心被逮的風險等
對於網路詐欺防制策略之認知	多久被查獲、查獲原因、從事網路詐欺之風險程度與風險因素、網路監控措施與網路詐欺行為之規避措施、獲利方法與手段、警察查緝能力之認知
概括問題	其他政府採行反詐欺預測策略之建議事項


假投資詐騙
高市刑大 偵五隊 偵破假投資詐欺水房案示意圖
1.老師;
2.助理;
3.小號;
4.水軍
LINE
飆股
詐騙集團
架設
假投資APP
以Line群組
誘使被害人投資
被害人匯款
人頭帳戶
詐騙水房
轉出贓款
投資平台拒絕出金
關閉網站
被害人
血本無歸

假網拍詐騙

內政部 警政署 刑事警察局 CRIMINAL INVESTIGATION BUREAU 165 Anti-fraud Hotline Service

歹徒於社群平臺張貼
販售各類商品貼文
吸引民眾洽談

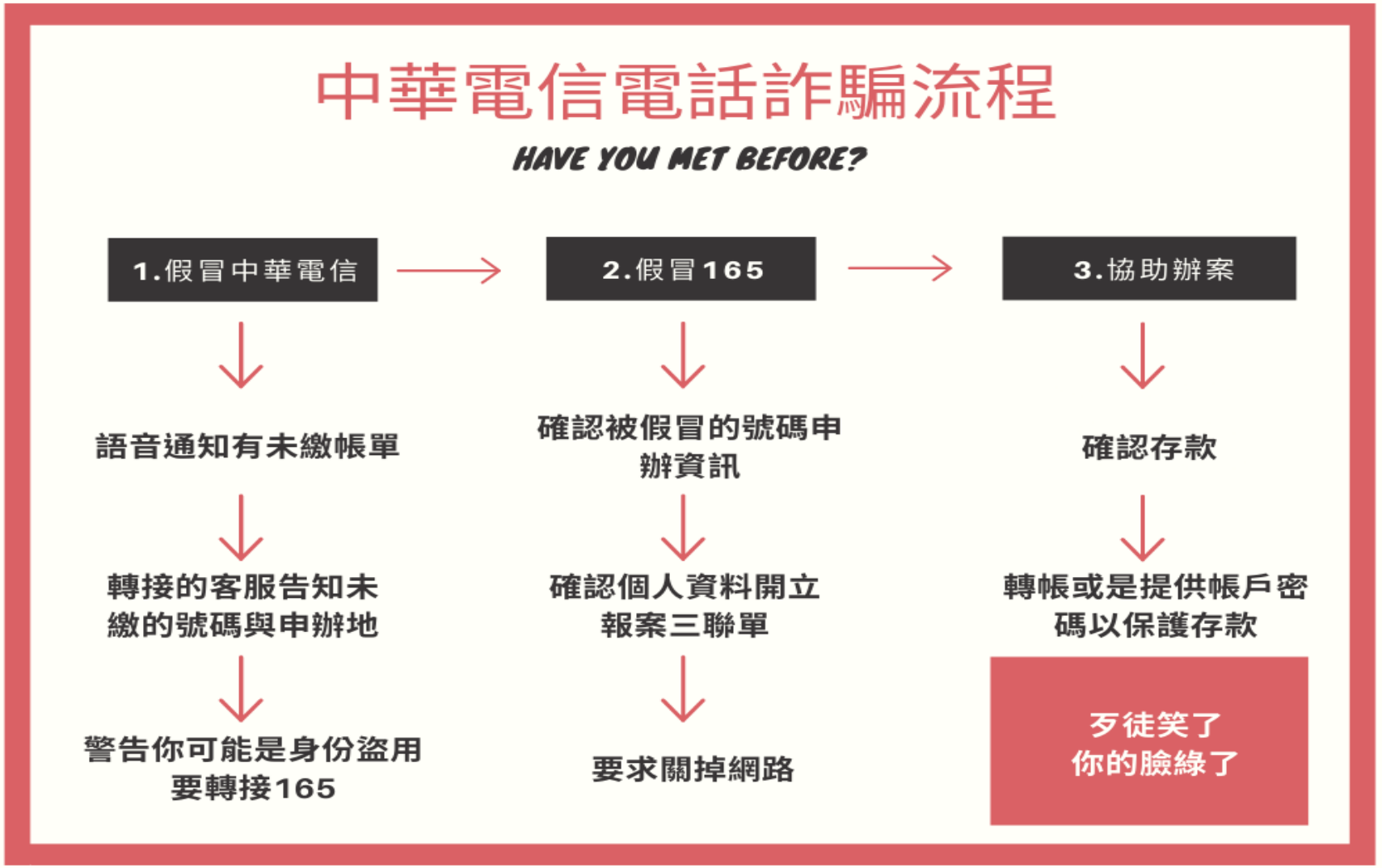
利用網路匯款、貨到付款、
LINE PAY、購買遊戲點數
等方式進行交易

付款後對方失去聯繫，
驚覺遭詐

利用社群平臺購物遭詐風險高

慎選優良商譽、提供第三方支付管道之拍賣平臺

假冒客服人員詐騙手法


中華電信電話詐騙流程
HAVE YOU MET BEFORE?
1.假冒中華電信
2.假冒165
3.協助辦案
語音通知有未繳帳單
轉接的客服告知未繳的號碼與申辦地
警告你可能是身份盜用要轉接165
確認被假冒的號碼申辦資訊
確認個人資料開立報案三聯單
要求關掉網路
確認存款
轉帳或是提供帳戶密碼以保護存款
歹徒笑了
你的臉綠了

網路詐欺加害者深度訪談分析

- 家境或經濟困頓、需求孔急、接觸詐騙集團成員。
- 大部分沒有詐騙被害經驗。
- 詐騙獲利豐厚，大多超出預期，利益薰心，難以抽離
- 網路詐欺之特性: 專業分工、部門間不具連結或互通性(部門間彼此不認識)、具有培訓機制、利用社群平台作為詐騙媒介。
- 被害者特性: 購物與投資以年輕者居多、解除ATM者以年長者居多；購物買賣糾紛以收入較低者多，投資詐騙者以收入較多且有一定資產者多，女性較多。
- 獲利方式大多是以抽取傭金方式進行。
- 對於警察的偵辦能力均予以肯定，並自認遲早會為警查獲
- 持續宣導以提高民眾防詐意識是有用的。

網路詐欺被害經驗與加害手法之比較分析

- 相同點:
- 1.被害人與加害人都是高度使用網路之族群
- 2.被害人與加害人都是使用網路上之社群媒體、購物網站以及從事線上遊戲作為網路生活之主要型態
- 3.被害交易方式主要以網路ATM轉帳、超商付款以及購買遊戲點數方式支付或交易
- 4.加被害兩造均不認識，透過網路平台的互動、交流成功詐騙
- 5.大多數的網路詐騙案件被害人與加害人都知道詐騙案件是否既遂

網路詐欺被害經驗與加害手法之比較分析

- 相異點
- 1. 被害者的人口特性與加害者之經驗不一致(類型不同)
- 2.被害者中有近7成選擇不報案；但加害者經驗則是認為被害者一定報警。
- 3.被害者不願意報警之原因之一為質疑警方之辦案能力；但加害者均肯定警察的辦案能力，認為遲早會被逮捕。

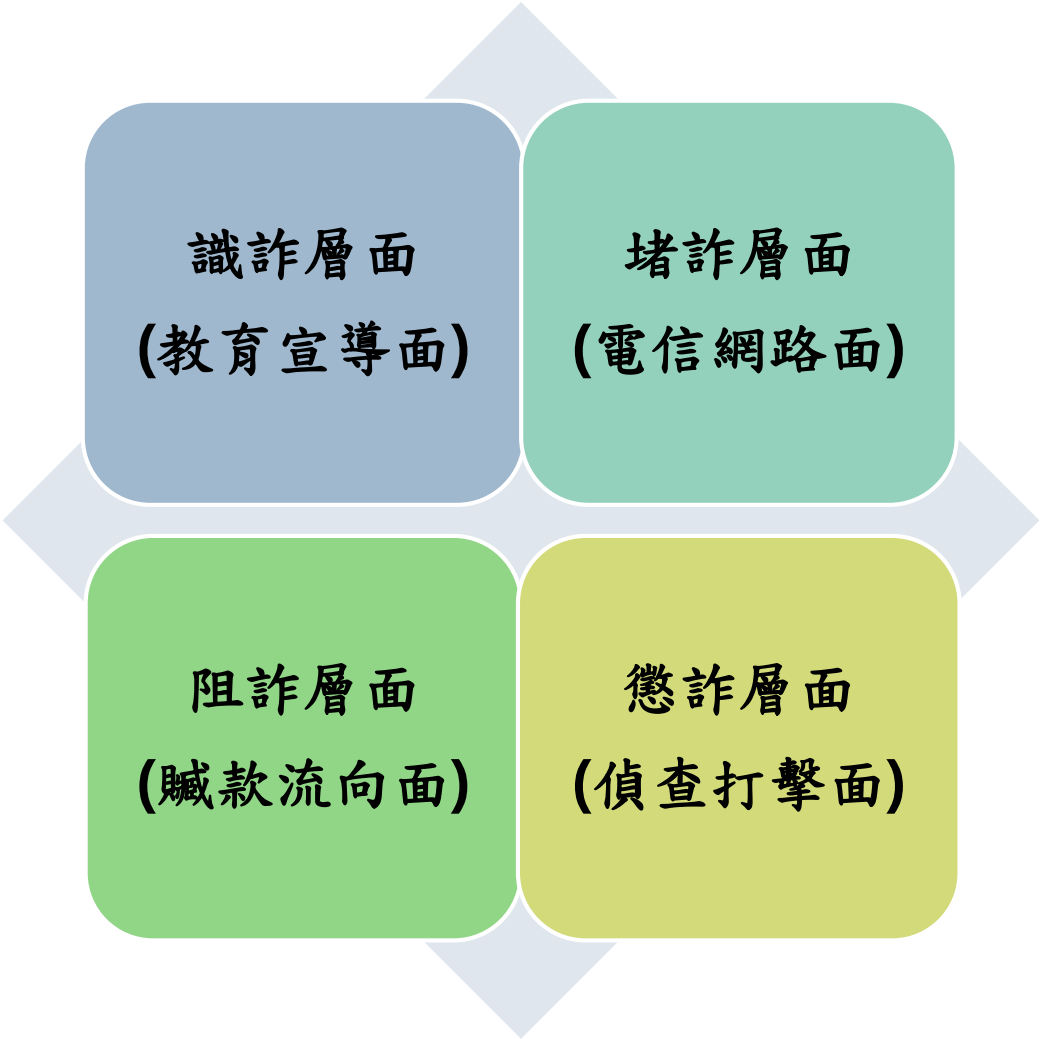
兩場焦點團體座談之人數及與會者背景

參加場次	相關領域	代碼	專家學者姓名	服務單位	討論主題
第1場次	被害者學	F1	OOO 博士	○○大學	網路詐欺之定義、型態、範疇，以及訪綱的妥適性
	網路犯罪與問卷設計	F2	OOO 博士	○○大學資管系	
	網路犯罪偵查警政	F3	OOO 大隊長	○○○警察局	
	網路犯罪偵查檢調	F4	OOO 檢察官	○○○地檢署	
第2場次	網路犯罪偵查檢調	F5	OOO 前檢察官/律師	○○○律師事務所	網路詐欺被害的防制對策，並討論有效的預防對策
	網路金融科技公司	F6	OOO 執行長	○○○網路科技公司	
	金融機構網路銀行資安負責人	F7	OOO 資安長	○○○銀行	
	科技犯罪偵查技術及網路鑑識	F8	OOO 博士	○○大學助理教授	
	網路犯罪偵查警政	F9	OOO 股長	○○○警察局	

政策焦點團體座談之討論大綱(第二場)

1. 從各國網路詐欺被害調查之管道與機制得知，有無值得借鏡之處？
2. 網路詐欺犯罪有無資訊/資安/理工等相關理論可解釋其行為或模式?
3. 從網路詐欺被害經驗問卷調查結果得知，被害人之心理特質與網路生活型態與其網路被害息息相關，請問被害人可以如何防範被網路詐欺被害？
4. 從網路詐欺犯罪加害者的深訪結果得知，執法部門可以從何處強化，以降低渠等犯案動機或減少被害人被詐機會？
5. 從網路詐欺犯罪被害者與加害者之心理特質與日常生活之相同與相異點分析，可否提供相關的抗制網路詐欺犯罪對策？
6. 晚近新加坡/中國等華人社會對於網路詐欺犯罪之抗制策略，是否有參考採之處?
7. 當前政府打擊詐欺犯罪之策略，是否應該針對不同類型(例如購物、投資與電信客服..)，提供不同的策略方式？
8. 行政院於今年5月成立專責之打詐辦公室，以強化當前打詐的編制，迄今有無相關成效？

政策焦點團體座談分析-困境與瓶頸



識詐層面(教育宣導面)

- 目前識詐教育，並沒有針對分齡分眾與網路詐欺類型，製作明確的防詐宣傳海報或影片，以提升民眾知能。
- 第一線執法人員的專業知能與執法技巧之精進與強化，也很重要。
- 近年來網路投資詐欺金額有增加趨勢，網路投資重複詐欺的個案也日趨嚴重，被害人甚至不願意承認自己已被詐騙，經過一段很長的時間後(例如兩個半月後)才報案；被害人數呈現出M型化的分布，亦即會被詐騙的人就是會一直被騙下去。

堵詐層面(電信網路面)

- 目前165打擊詐欺專線僅是內政部警政署刑事警察局下一個股的層級，與其他部會溝通、協調並請求支援，甚至跟民營機構溝通、交涉，位階過小，能力有限。
- 因為「數位中介法」沒有通過立法，許多網路詐欺犯罪之行為就無法監控，對於堵詐限縮其效能。
- 運用高科技，甚至運用AI技術來提升科技辦案以堵住網路詐欺犯罪，仍嫌不足。
- 犯罪嫌疑人將整個網路詐騙行為予以分工，乍看之下各自獨立，司法實務也會認為無具體證據證明渠等為網路犯罪集團或組織，無法起訴。
- 網路平台業者未能負起審查廣告內容的責任。

阻詐層面(贓款流向面)

- 政府與產業合作的量能與授權的業務，似乎仍嫌過少，因為產業界也希望與政府合作建立防護網，阻斷詐騙集團的金流。
- 台灣偵查網路詐欺犯罪，特別是運用區塊鍊、加密貨幣進行金流資產的轉移部分，阻詐能力仍嫌不足。
- 許多詐騙案都沒有人知道，所以也沒有辦法介入，但唯一例外是金融機構或銀行，而目前銀行的介入已經很積極，但似乎可以再強化。
- 目前針對不同網路詐欺型態，例如投資詐騙與網拍詐騙，手法、金額與詐騙期間都不同，其防制策略應該有所不同

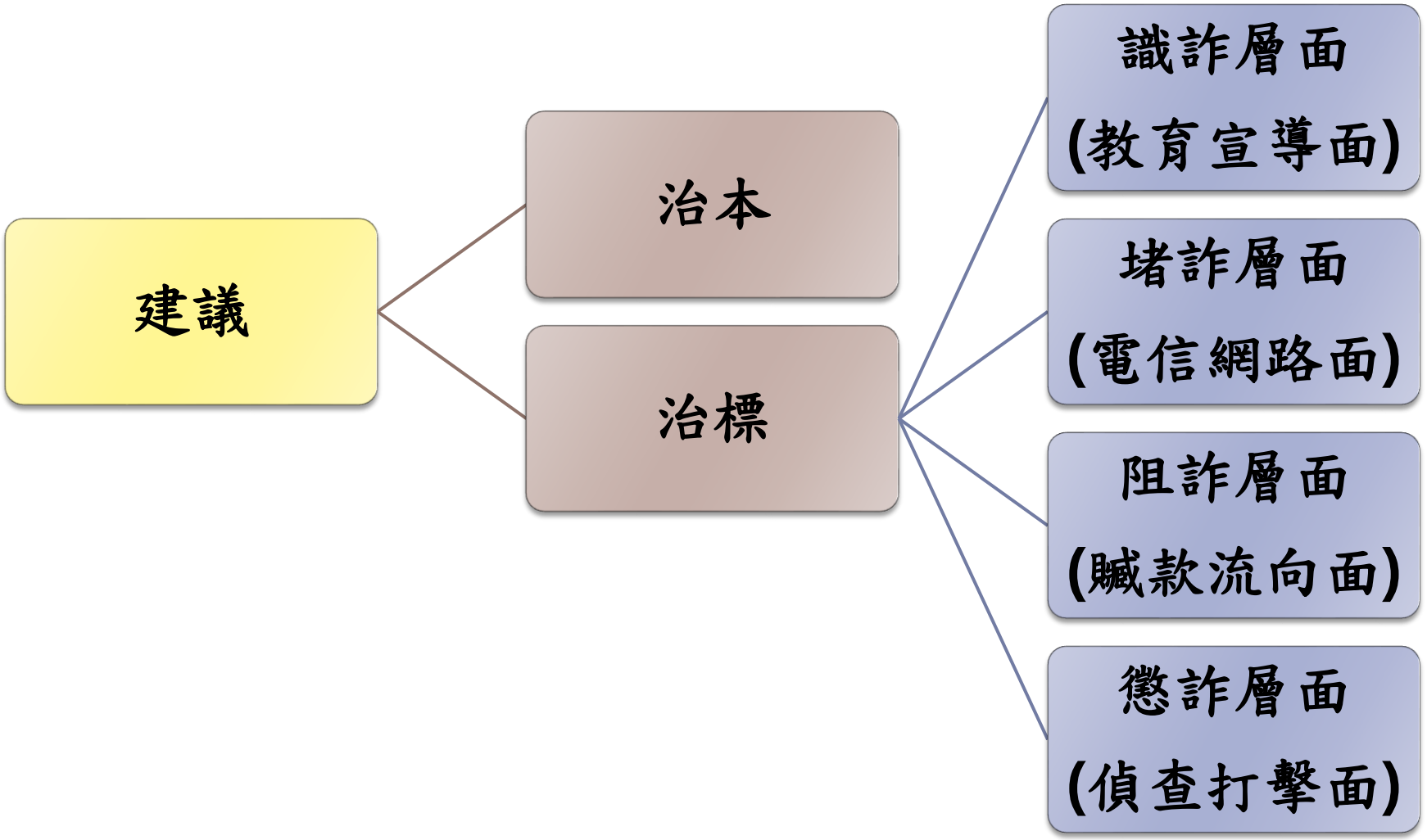
懲詐層面(偵查打擊面)-1

- 跨國跨境的司法互助很重要，但目前的司法互助大都鎖定檢察官層級，曠日廢時，且徒勞無功。
- 目前我國派駐各國的警察聯絡官，在扮演跨境查緝網路詐欺案件的角色，非常吃重，人力與據點因隨著詐欺集團的擴散而增加。
- 與跨境跨國的警務部門之合作很重要，如果關係緊密者，請求其回覆協查的資訊就很快，反之就很慢，甚至石沉大海。
- 目前政府欠缺網路詐騙案件專家鑑定的機制，可以彌補警方在科技偵查上的不足。
- 雖然通過「打詐5法」，但根據過往經驗，法院在裁處方面可能沒辦法有效的落實，以達嚇阻功效。

懲詐層面(偵查打擊面)-2

- 專責偵辦單位，目前政府所提供的資源有效，且橫向連結不足、金融機構基於保護個資也不願配合提供相關資料，造成偵辦網路詐欺案件常存在斷點的現象。
- 網路詐欺犯罪有其模式與伴隨一些網路媒介的普及有其盛行性，比如說之前Telegram流行大概2、3個月，詐騙模式與手法就會一直變。造成我們執法人員一直在後追趕其行為模式，在防堵上也比較難對症下藥。
- 不僅第一線執法人員在網路詐欺犯罪的執法量能不足外，現行懲罰力道不夠強、無嚇阻性，導致很多詐騙犯容易再犯。而過往「竊盜犯贓物犯保安處分條例」規定，對於犯罪人除科以刑罰外，還附加強制工作，但被宣告違憲後(釋字第812號)，刑罰之威嚇效能大為降低

建議



治本策略

- 網路詐欺與被害型態變動快速，須及時掌控方能有效防制
- 針對可能導致網路詐欺被害的誘因與動機，提供示警機制
- 強化民眾對網路成癮之認知，並提供成癮者及其家庭協助
- 針對有創傷症候群之詐欺被害人，提供心理輔導和社會支持
- 政府應定期且常態性地進行網路犯罪被害經驗之調查

治標策略-試詐層面(教育宣導面)

加強網路防詐觀念和技巧，提高被害人自我防護能力

網路詐欺被害高風險族群進行分群分眾犯罪預防宣導

犯罪預防宣導保證獲利的字眼，應屬詐騙宣傳手法

治標策略-堵詐層面(電信網路面)

- 盡速制訂與通過防制詐欺犯罪(如科偵法)之相關法律
- 仿照毒品犯罪制定「詐欺犯罪防制條例」專法
- 應於行政院層級設置詐欺犯罪防制中心

治標策略-阻詐層面(贓款流向面)

- 應與公私立金融資訊機構建立資安互助合作機制
- 建立跨國跨境警務偵查互助合作平台
- 簽署保全電子證據之國際協議與協定
- 仿照新加坡模式應由金融主管機關主導情資交換

治標策略-懲詐層面(偵查打擊面)

- 強化網路詐欺之查緝，並提升民眾對執法機關之信心
- 強化165專責打擊詐欺犯罪中心之部門與陣容
- 根據網路詐欺犯罪熱點與移動適時增加境外警務人員
- 第一線執法人員之定期專業教育訓練
- 科偵部門應該運用AI或大數據進行犯罪手法分析
- 提高網路詐欺犯罪者懲罰之刑度或提高量刑

報告完畢

敬請指教