



111 年 3 月政風小品集廉政宣導篇

廉政交流網



法務通訊
第 3090 期
2022 年 1 月 14 日

尊重生命課題 守護民眾權益 政風與您同在

殷吉慧 臺南市下營區公所政風室主任

壹、前言

近年來，雖然因為殯葬文化之漸趨多元，民眾對於土葬或火葬之傳統意識選擇略有改變，惟慎終追遠則依然是民俗傳統美德。生死既是必然，在面臨高齡、少子化社會等趨勢下，殯葬設施之設置管理，既有其重要及必要性，且與生活息息相關。

就殯葬禮儀而言，重視生命之尊嚴與價值，不僅係尊重亡者，更能撫慰生者，使生死兩相安。臺南市下營區公所秉持上述之理念，於 108 至 109 年間，就區域內納骨堂蓮華園，設計增設納骨塔櫃位，並以「尊重逝者、體恤生者」為規劃原則，期許提供區民最完善的殯葬設施。

貳、預警作為之緣起

緣臺南市政府民政局執行臺南市殯葬事業管理基金補助經費，由下營區公所辦理「下營區納骨堂二樓增設納骨櫃工程」。辦理期間，原得標廠商即因材料送審資料不全及分批進料等多項因素，而經歷數次修正，並因此延緩材料廠驗等程序，導致工程

進度延緩；期間，下營區公所政風室會同農業及建設課同仁、廠商及設計、監造單位至指定工務處所進行廠驗及材料試驗等應行程序，發現廠商履約情形具有顯著延緩及異常，爰經研擬數項建議作為供業管單位處辦。後續則仍因廠商進度大幅落後且遲未改正，經研判履約能力不足，為避免爭議持續擴大，爰經下營區公所依規定辦理契約終止。

參、預警作為之建議

本案辦理過程中，下營區公所重行檢視全案辦理進程，除發現可歸責於廠商而導致進度嚴重落後之原因，並因此認定其履約能力不足，為免延宕情形嚴重損害民眾權益，導致公所行政效率遭受質疑及影響民眾權益，政風室提列下列建議供業管單位參處：

- 一、要求廠商儘速排定工程廠驗期日，確保產品原產地屬於我國，並確實要求廠商提送趕工計畫書及敘明預施作進度與明確數據。
- 二、工程廠驗之材料送審作業延宕工期，其計算應



廉能是政府的核心價值，貪腐足以摧毀政府的形象，
公務員應堅持廉潔，拒絕貪腐，廉政檢舉專線 0800-286-586



新北市政府交通事件裁決處政風室 關心您!!

妥慎考量是否應歸責廠商，同仁催辦事宜，亦應確實製作公務電話紀錄或書面資料謹慎保存。

三、爾後類案，如有工程落後達相當比例者，應定期辦理工程進度檢討會，於必要時並要求提送明確之趕工計畫，以加強類案之履約管理。

四、修訂相關規管、非明文作業規定以供類案辦理情形參採，並研議將相關會議流程透明化，以避免履約爭議及增進效能。

其次，下營區公所經與原得標廠商終止契約後，立即重新辦理採購作業程序，並於相關會議、材料審查及廠驗作業後開工進行，後續並研議再行增加384櫃位，總數達1,664個櫃位，經申報臺南市政府民政局核定後均已完成設置及啟用。

肆、預警作為之達成效益

一、避免工程品質不彰損害民眾權益

本案經於廠驗及工程檢討會等程序中，發現廠商提供之材料品質不佳，相關料件亦有鏽蝕情形，且保管情形均有不妥，蓋因納骨塔櫃位之設置，係先人受祭祀神聖及莊嚴之器物，本案經及時預警，有效避免後續可能之工程闕漏，導致區民權益受損及爭議擴大。

二、有效擷節公帑，強化標案執行能量

全案經與原得標廠商終止契約後，下營區公所據依原契約內容沒收履約保證金及差額保證金等款項共計新臺幣51萬2,180元，並據相關建議措施妥適修訂契約內容辦理採購作業，後續並增加納骨櫃位之設置，除有效節省公帑，亦確實保障了民眾權益，有效強化標案執行能量。

三、避免民眾怨懟

按納骨堂增設納骨櫃工程，其工程施作品質之要求，係為提供民眾更好之追思環境及解決祭祀需求，與民眾權益相關，亦為政府施政滿意度之重要一環，本案即時預警，防堵爭議孳生，有效避免民眾怨懟。

四、有效策進提升實際防弊效能

為傳承本案執行經驗，案經提報於下營區公所109年廉政會報，會中研議將材料審查會議流程透明化並據以實行，後續確實邀集承攬廠商及設計監造單

位共同至該所會議室公開辦理材料送審審查會，確實加速審查及避免履約爭議，效益良好。

五、鼓勵同仁勇於任事

辦理過程中，政風室均提醒承辦同仁，將相關聯繫催辦過程確實書面化記錄，以維護自身權益，全案經辦理完竣，考量業務單位及時預警處置，有效避免民眾權益受損及公帑之浪費，辦理過程辛勞且確具績效，爰經主動簽請公所考績委員會研議核予相關人事獎勵在案，藉此鼓勵同仁勇於任事。

伍、結語

正所謂「生，事之以禮，死，葬之以禮，祭之以禮」。殯葬文化之維護涉及民眾之重大權益，爰此，公部門對於納骨塔櫃位之設置更不可輕忽，下營區公所秉持資源有效運用、錢務須用於刀口等基本原則，於辦理本案採購作為中，以數項有效、確實之預警處置作為，避免工程產生爭議，期能提供民眾完善之祭祀空間。

攝影風情

飛



楊緒牧 臺灣高等檢察署退休同仁



111 年 3 月政風小品集機密維護篇

法務部調查局《清流》雙月刊---淺談資通安全最弱環節



想要看到月刊更多專欄：

<http://mjib-ebook.com/MJIB/no37/index.html>

文章
往下
翻閱

廉能是政府的核心價值，貪腐足以摧毀政府的形象，
公務員應堅持廉潔，拒絕貪腐，廉政檢舉專線 0800-286-586

新北市政府交通事件裁決處政風室 關心您!!



你夠在意嗎？ 考驗人性的社交工程誘惑

◆ 社團法人臺灣E化資安分析管理協會、逢甲大學創能學院 — 林子煒

社交工程形形色色，若不夠留意，駭到你會怕。

社交工程—— 駭客最有效且省錢之攻擊方式

自從人們可以利用網際網路互通有無，每個人至少都擁有多個網路服務帳號，包括個人或其所屬單位的電子郵件帳號；正因如此，利用資訊科技便利之社交工程犯罪行為層出不窮，且趨勢逐年上升。

社交工程即為人與人之間的攻擊。過去關於此類攻擊定義為「攻擊者藉由社交手法取得系統或網路的資訊」，然而現今攻擊者的目標，已逐漸轉到個人擁有之資訊。此攻擊管道，最常見的為電子郵件、簡訊、即時通訊軟體（如 Messenger、Skype、Line、Instagram、Whats App）等

等。為何此種攻擊趨勢會逐年上升？因為對駭客而言，這是最有效、最省成本的攻擊方法。

親身經歷之詐騙案例

以自身經驗為例，某天上午收到親戚 X 寄來的英文信，信中述說他「正在英國旅遊，但被當地歹徒持槍威脅交出身上所有財產，包括金錢、信用卡、行動電話等。這封信是透過當地的免費網路寄出，現在急需金錢援助，請用西聯匯款（Western Union）匯 2,350 英鎊（約新臺幣 9 萬元）給我」。

信中附上姓名與地址，我抱著好奇心利用 Google 地圖查詢，結果發現那家英國旅館竟然地處在杳無人煙的社區。另個親戚 Y 也在詢問是否有收到這封信，所以我們研判親戚 X 的信箱帳戶應該已被盜用，而盜用者寫了這封信，並寄給信箱內所有的聯絡人。

詐騙者指定西聯匯款¹的原因，係因其匯、收款的雙方都不用開設銀行帳戶，只要填寫雙方英文姓名與出示身分證明即可匯款。作法是在匯款人填妥表格後，系統會產生一組 10 位數密碼，匯款人只要將



筆者收到透過親戚 X 信箱寄來的詐騙電子郵件（左），聲稱遭到搶劫急需金援，要求以不用開設銀行帳戶的西聯匯款（右）轉匯。（圖片來源：作者提供）

<p>西聯卡持有者請填寫卡號 For Western Union® Cardholders, please fill in your card number.</p> <p>卡號 Card No. <input type="text"/></p> <p>金額 Amount <input type="text"/></p>		<p>西聯卡持有人，如原先提供的資料沒有變更，僅需填寫標示綠色部份 For Western Union® Card holders, please fill in the green highlighted areas only, unless any of your details previously provided to us have changed.</p>
<p>目的地（城市及國家）Destination (city, country)</p> <p>金額（正楷大寫）Amount (in words) <input type="text"/></p>		
<p>收款人 (Receiver)</p> <p>名 First name(s) <input type="text"/></p> <p>姓 Last name(s) <input type="text"/></p> <p>父姓 (Paternal) <input type="text"/> 母姓 (Maternal) <input type="text"/></p>		
<p>匯款人 (Sender)</p> <p>名 First name(s) <input type="text"/></p> <p>姓 Last name(s) <input type="text"/></p> <p>父姓 (Paternal) <input type="text"/> 母姓 (Maternal) <input type="text"/></p>		
<p>地址 Address <input type="text"/></p> <p>街名和門牌號 (Street) <input type="text"/></p> <p>城市 (City) <input type="text"/> 省/國家 (Province/Country) <input type="text"/> 郵政區號 (Postal Code) <input type="text"/></p>		
<p>聯絡電話/Telephone no. (<input type="text"/>)</p>		
<p>另外收費的服務選項。請勾選需要的服務項目 Optional Service available at additional cost. Check service desired:</p> <p><input type="checkbox"/> 我需西聯匯款支票或現金形式寄人發送給收款人，送地址如下。 I want a check/money delivered to the following address:</p>		
<p>地址 Address <input type="text"/></p> <p>街名和門牌號 (Street) <input type="text"/></p> <p>城市 (City) <input type="text"/> 省/國家 (Province/Country) <input type="text"/> 郵政區號 (Postal Code) <input type="text"/></p> <p><input type="checkbox"/> 我需西聯用電話通知收款人 I want Western Union to telephone the Receiver. (<input type="text"/>)</p> <p><input type="checkbox"/> 附加留言 Message to be sent: <input type="text"/></p>		
<p>對於匯款金額低於1,000美元且收款人無有效身份證件，請填寫驗證問題及答案。 When sending less than USD \$1000 and the receiver does not have valid identification, complete the Test question and answer: (The maximum amount that can be picked up without I. D. is USD \$1000.)</p> <p>收款人是否有有效身份證件? Will the Receiver have valid identification?</p> <p>有 Yes <input type="checkbox"/> 沒有 No <input type="checkbox"/> 如果沒有請提供驗證問題。 If no, provide a Test Question: (限4個英文字 Limit 4 Words)</p> <p>驗證問題 Question <input type="text"/> 答案 Answer <input type="text"/></p>		
<p>匯款性質 Nature of Remittance <input type="text"/></p>		

¹ 成立於 1851 年，號稱是世界最大的電子匯款公司，在全球超過 200 個國家與地區設置至少 21 萬個據點，提供各地收、匯款服務，
<https://www.westernunion.com/us/en/home.html>。

密碼給收款人，收款人就能憑藉英文姓名及密碼進行提款。時至今日，全球已有相當多利用西聯匯款而被詐騙的案例，警方與銀行都無法追蹤及攔截詐騙款。

社交工程郵件之包含要素

以電子郵件來詐騙至少已有十年歷史，然至今仍有民眾上當，因為民眾輕忽或無知，易讓駭客達到欺騙目的。社交工程電子郵件不乏利用聳動的郵件主旨、偽造受害者熟悉的寄件者、以假亂真的郵件內容等等，試圖吸引使用者上鉤。社交工程電子郵件中會有幾個要素，包含超連結、附件、圖片、郵件內容內嵌程式碼。

-  **超連結：**有可能會讓受害者連至攻擊者所架設之惡意網站，藉此收集受害者相關資訊。
-  **附件：**多含惡意程式，開啟並執行後會潛藏在受害電腦裡，直接將電腦內資料對外傳輸、偷偷側錄用戶使用電腦的任何行為、接續下載惡意程式至受害電腦再執行各項行為等。
-  **圖片及郵件內容內嵌程式碼：**能回報給攻擊者表示「登陸成功」，更甚者直接讓受害者電腦自動從中繼站下載小程式（諸如鍵盤側錄工具、

螢幕側錄工具等），記錄受害者使用電腦行為，再進行下一步攻擊。

以上要素不一定會同時出現，亦可能交互搭配使用，曾有僅憑單一內容即欺騙成功的案例，造成受害者損失。例如，假冒會議邀請信函，成功欺騙到受害者出門參加會議，加害者利用這段時間闖空門等。

勒索軟體通常包裹著社交工程郵件外衣

近幾年造成全球重大災情的勒索軟體，大部分行為模式即透過社交工程電子郵件，讓受害者點擊後自動下載並執行一個看似無害的小程式，連線至外部中繼站下載勒索軟體主程式，此主程式會開始掃描電腦所存文件²後加密，跳出警告訊息，指示受害者利用比特幣付款至指定帳戶以換取解密提示。

日本年金機構之個資外洩事件

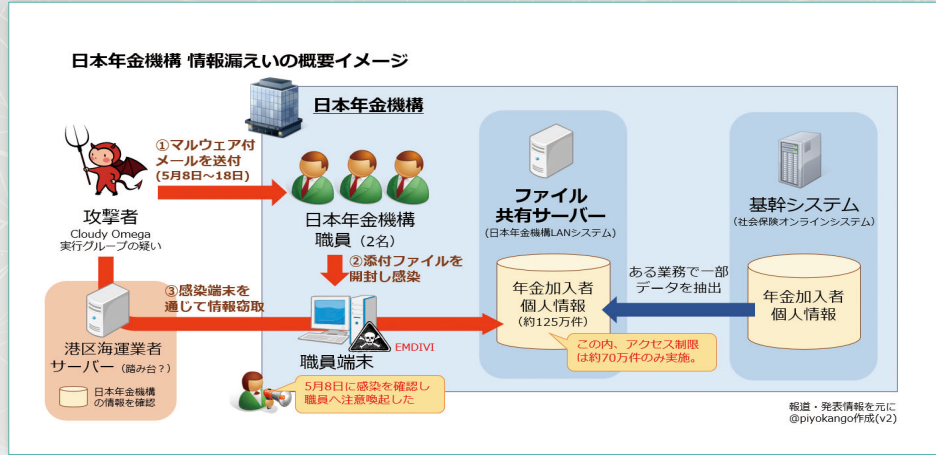
若讀者認為，就算有人「運氣這麼不好」開啟了社交工程電子郵件，造成傷害也不過是個人財產及聲譽。其實損失的嚴重性，絕非想像中的那般簡單。

掌管日本全國國民年金的組織「日本年金機構」（相當於勞動部勞工保險局國

² 多為 Office 系列，以及 PDF 或 JPEG 圖檔等企業常見之檔案格式。



大部分勒索軟體的行為模式，即是透過社交工程電子郵件誘惑使用者點擊，而成為受害者。



日本年金機構個資外洩事件示意圖，遭駭主因係員工不慎打開含病毒之社交工程電子郵件所致。（Photo Credit: piyokango, <https://piyolog.hatenadiary.jp/entry/20150601/1433166675>）

民年金組），於 2015 年 6 月召開記者會，坦誠因員工電腦受駭客攻擊，導致民眾個人資料外洩³；整起事件的起因，即為員工不慎打開含病毒之社交工程電子郵件所致。

剛開始是該機構九州分部員工收到社交工程電子郵件，點選超連結後，即被自動下載惡意程式，並開始不正常的電腦連線。

雖然日本國家網路安全中心（National Information Security Center, NISC）⁴ 於第一時間發出通報，但因為日本年金機構檢測不出原因，因此僅更新個人電腦的防毒軟體，直到東京本部也有員工收到同樣的社交工程電子郵件並開啟，偵測到儲存年金的資料庫有異常連線行為後，才驚覺事態嚴重。日本年金機構事後雖通知警方，

且 NISC 亦緊急派員處理，然已造成所屬 5 個單位內有多達 19 臺的個人電腦遭受感染，最後清查出來竟然有高達 125 萬筆的個人資料外洩，嚴重影響到仰賴年金度日之日本民眾的生活。

社交工程之攻擊方式

由日本年金機構案例可知，只要個人一時疏忽，即使只是小小電子郵件，就有很大的機會對企業、群體，甚至國家安全造成危害。

另外，即時通訊軟體也成為社交工程攻擊管道之一。在 COVID-19 疫情高峰時，國內採取口罩預購制，意外出現「口罩釣魚簡訊」，佯稱口罩到貨，引誘使用者點擊簡訊

³ 《病毒入侵！日本年金機構 125 萬個資遭外洩》，<https://news.ltn.com.tw/news/world/breakingnews/1335620>。

⁴ 是日本負責網路危機應變處理之政府單位，為 2015 年 1 月由「內閣官房資訊安全中心」升格而成，代表將網路安全提高到國家安全層次。

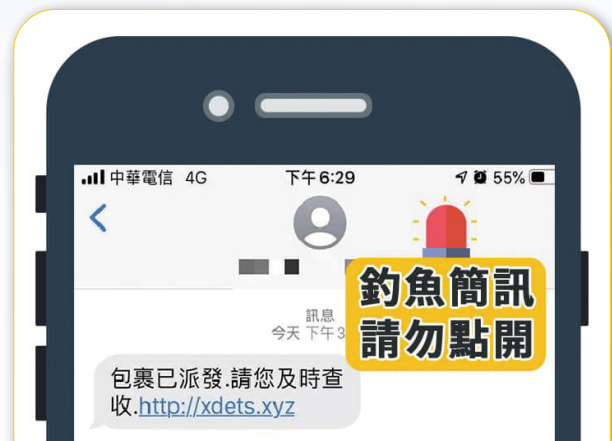
內連結，當時亦有不少臺灣民眾受駭⁵。以下再列舉其他社交工程之攻擊種類。

- 一、**濫發電子訊息**：諸如惡意電子郵件、釣魚簡訊、即時通訊等文字訊息。此類攻擊通常一次廣發給多名使用者，因此亦稱為「垃圾郵件」。
- 二、**釣魚**：此類攻擊通常會讓使用者「信以為真」，透過話術讓人誤信，進而騙取錢財。近期常見「假交友」、「假投資」即屬此類。
- 三、**願者上鉤**：經典手法為攻擊者在公司門口隨意丟棄一個隨身碟，該公司不知情員工撿到後，誤以為是公司內有人不小心遺失，為了順利歸還，故而將該隨身碟插進自己的電腦內，殊不知惡意程式就此開始執行。
- 四、**搭順風車**：尾隨員工進入外人不該進去的區域，進而竊取到公司內部機密資訊。
- 五、**水坑攻擊**：利用網頁藏惡意程式碼的方式，讓使用者的電腦中毒。只要入侵或偽造目標受害者常瀏覽的網站，植入惡意程式，當受害者瀏覽該網站，即會下載惡意程式。

社交工程攻擊之防範措施

社交工程攻擊防不勝防，面對攻擊，可行的防範措施包含：

- 一、**使用垃圾郵件過濾器**：現行的郵件伺服器（包括 Gmail）皆有此機制。
- 二、**定期更新**：隨時更新防毒軟體、防火牆與電腦及手機的作業系統，以防任何安全性漏洞被利用。
- 三、**仔細確認**：確認訊息與自己是否相關，並查證訊息來源，有必要時打電話向來源確認。



釣魚簡訊經常引誘使用者點擊簡訊內連結，進而竊取民眾個資、詐騙錢財。（圖片來源：內政部 FB 粉絲專頁，<https://www.facebook.com/moi.gov.tw/photos/a.1053616048000131/3275894322438948>）

⁵ 《台灣詐騙網址暴增 4 倍 駭客冒用口罩預購行騙》，<https://www.cna.com.tw/news/ait/202009220313.aspx>。



人是最大的零日漏洞，只要使用者資安意識稍有不足，即為攻擊者打開一扇自由進出的大門。

四、提高警覺：個人應提防不明電子郵件，並且勿任意點選附檔及超連結。

人是最大的 Zero-Day

社會生活中形形色色的誘惑，即是社交工程對於網路用戶的最佳詮釋，諸如「清不完的木馬，無知與恐懼也；補不完的系统，人腦也」、「人是最大的 Zero-Day⁶」等，雖然只是玩笑話，也道出了防範社交工程的最關鍵要素是「人」。資訊技術發展這麼多年，為何電子郵件社交工程依然是攻擊者的攻擊手段首選，乃因為電子郵件是阻力最小的攻擊路徑，只要使

用者資安意識稍有不足，開啟惡意電子郵件，即為攻擊者打開一扇自由進出的大門，也開闢了一條讓使用者或其所屬組織邁向毀滅的道路。因此，在日常生活中一定會接觸到電子訊息的我們，勢必要多加瞭解是類攻擊，且必須養成習慣、提防不明電子訊息。相信你只要夠「在意」，必當能防範形形色色且誘惑人性之社交工程攻擊。



社團法人台灣 E 化資安
分析管理協會 (ESAM)

⁶ 在電腦領域中，零日漏洞或零時差漏洞 (zero-day vulnerability、0-day vulnerability) 通常是指還沒有修補程式的安全漏洞，而零日攻擊或零時差攻擊 (zero-day exploit、zero-day attack) 則是指利用這種漏洞進行的攻擊。「零時差漏洞」是軟體或硬體的瑕疵，如未能及時修補，駭客就能在未被察覺的情況下透過網路侵犯個人隱私、偷取商業機密與摧毀公共設施等。



111 年 3 月政風小品集安全維護篇

醉後搭捷運 捷運警察呼籲為了安全要量力

2022 年 2 月 11 日 記者方笙楠臺北報導

臺北捷運系統為雙北地區重要大眾運輸工具，亦為一般民眾聚餐飲宴後交通工具首選，惟偶有旅客不勝酒力而醉倒於捷運系統內，輕則迷路，重則因身體失衡碰觸其他旅客導致糾紛等情，抑或在站內咆哮等脫序行為，經臺北市政府警察局捷運警察隊數據統計，去年受理酒醉旅客案件共 162 件，站內咆哮等脫序行為即有 49 件，占 30% 為最多、與人發生糾紛者亦高達 24 件，占 15%，數量驚人。

捷運警察隊員警日前巡經捷運南港展覽館站，乍見一名女性旅客額頭有撕裂傷坐臥地上，經了解係因不勝酒力，獨自搭乘手扶梯時重心不穩跌倒所致，幸經捷警通報救護人員，並聯繫其友人帶回後無大礙；另於 111 年初亦曾接獲捷運善導寺站月臺有民眾酒醉咆哮情形，捷運警察隊第三分隊警員李恪明、林萬慶到場後只見一名中年男子胡言亂語、答非所問，甚於陪同該男子如廁時，男子因泥醉到無法自己拉上拉鍊，還需由捷警代勞！而今年截至 1 月底，捷運系統旅客因酒後失去言行控制能力，脫下口罩遭開罰之案例也已達 4 件，當事人原為避免酒駕搭乘大眾運輸，卻因飲酒過量而變調。

臺北市政府警察局捷運警察隊呼籲，近期適逢公司行號舉辦年節春酒等聚會，民眾若有飲酒，宜謹慎評估自身體力及精神狀況適量飲酒，尤其捷運系統內多設有手扶梯、階梯，常有高度落差較大之情形，為確保自身安全並避免造成其他旅客困擾，飲宴後建議可由「親友陪同搭乘捷運」，或採「指定親友駕駛」、「酒後代為駕駛」及「代叫計程車服務」等 4 項作為；如看見他人酒醉需協助情形，可即時向捷運警察、站務人員、保全反映，於車廂中可按壓緊急對講機求助，捷警獲報將即趕赴現場處理，以保旅客安心乘車。

資料來源：民眾網民眾日報



111 年 3 月政風小品集消費者保護篇

為半自動點擊調切換控制 消保官提醒易誤觸刷臉付費

2022 年 2 月 4 日 記者謝東明/台北報導

只需簡單一瞥，Face ID 便可讓您安全地解鎖 iPhone 或 iPad、認證購物交易、登入 App 等。



記者翻攝自 APPLE 官網

新冠肺炎 Omicron 變種病毒疫情再起，春節年假期間不出門拜年，宅在家中玩手機遊戲的情形將更加普遍。新北市政府消費者保護官提醒，消費者除了要控管好手機的付費功能不被他人盜用，更要留意新款 iPhone 的「Face ID」（俗稱刷臉）付費及「切換控制」功能。玩手機遊戲如果為了「半自動點擊」而使用「切換控制」功能，稍一不慎就可能完成刷臉付費，而引發交易糾紛，玩家千萬要注意。

消保官表示，新款 iPhone 手機有所謂「切換控制」功能，有行動障礙的使用者可以透過「切換控制」的輔助使用功能選擇、點按、拖移、輸入文字，甚至可



以自訂許多手勢的組合。

但不少手機遊戲玩家發現「切換控制」功能，可以設定為「半自動連續點擊」，例如在「抽獎」的位置連續點擊 20 下並完成錄製，按側邊按鍵 3 下啟動「切換控制」功能後，進入抽獎頁面只要點 1 下，就會在抽獎位置自動點擊 20 下，可以立即完成 20 次抽獎。

這種「切換控制」功能，雖然可以省去玩家大量的點擊動作及時間，但也有風險。因為 Apple Pay 的刷臉付費確認機制是按側邊按鍵 2 下，如玩家進入付費頁面突然想啟動或關閉「切換控制」功能時，在按側邊按鍵 3 下完成切換之前，就已經完成刷臉付費的確認動作。

消保官指出，有玩家使用「切換控制」功能，連續「拉霸」，但發現亂點到購買商品的頁面，他按側邊按鍵 3 下想先關閉「切換控制」的功能，但沒想到按第 2 下時就完成刷臉付費，購買了 1000 多元遊戲點數。

玩家立即向 iTunes 平台請求退費，強調是誤觸且點數完全未使用，但業者則強調「切換控制」功能，主要是提供肢體不便或視覺障礙用戶使用，不建議一般用戶於手機遊戲使用，且 iTunes 是位於愛爾蘭的公司而非美商蘋果電腦股份有限公司，經連繫後 iTunes 無法同意退費。

消保官強調，通訊科技進步固然帶來許多使用上的便利，同時也伴隨風險，但這些功能其實都可以在設定選單中關閉，呼籲消費者應特別注意此類設定，以免因設定或操作不當而發生預期外的金錢損失。

資料來源：CNEWS 匯流新聞網



廉能是政府的核心價值，貪腐足以摧毀政府的形象，

公務員應堅持廉潔，拒絕貪腐，廉政檢舉專線 0800-286-586

新北市政府交通事件裁決處政風室 關心您!!



111 年 3 月政風小品集反詐騙篇

詐騙集團出新招「稱民眾被匡列」騙個資 指揮中心教 1 招反制

2022 年 1 月 18 日 王德蓉

近日本土疫情升溫，人心惶惶，沒想到詐騙集團竟又出新招，假冒衛生局來電宣稱民眾被匡列接觸者名單當中，以騙取個資，刑事局提醒若接到類似來電，可撥打「1922 防疫達人」或是警政署 165 反詐騙專線查證，指揮中心也傳授一招反制對方。

內政部警政署刑事局指出，鑒於近期 COVID-19 疫情升溫，有詐騙集團假冒警察局或衛生局，以疫調名義稱民眾被匡列在接觸者名單當中，要民眾提供全家人的個資，包括名字、生日、身分證字號、家庭成員等，再伺機誑騙民眾匯款或盜刷信用卡。

刑事局指出，依據 165 反詐騙專線資料，自 110 年 12 月至本（111）年 1 月 16 日止，民眾進線諮詢、檢舉或報案共計 14 件，尚無財損發生，同時也提醒民眾接到類似電話，對方稱自己是警政或衛生單位，可以詢問來源及其名字，稍後自行去電「1922 防疫達人」或是警政署 165 反詐騙專線查證。

指揮中心也提醒，不會向民眾詢問銀行帳戶、身分證字號等，更不會要求匯款、保管帳戶，民眾應特別注意，接到類似電話也可以反問對方「我的接觸者是誰」，辨識真偽。



有詐騙集團假冒警察局或衛生局，以疫調名義稱民眾被匡列在接觸者名單當中，騙取個資。（示意圖 / pixabay）

資料來源：周刊王 CTWANT



廉能是政府的核心價值，貪腐足以摧毀政府的形象，

公務員應堅持廉潔，拒絕貪腐，廉政檢舉專線 0800-286-586

新北市政府交通事件裁決處政風室 關心您!!