No. 177
Nov. 2021

政風電子報

【封面故事】
淺談資通安全最弱環節

【公務機密】
涉洩密給殯葬業，11警消遭訴

【廉政案例】
國安局退訓男PO文洩密 檢起訴求重刑

【人權宣導】
與惡的距離

【資安宣導】
臉書公布大當機始末報告：日常維護出錯所引發的骨牌效應

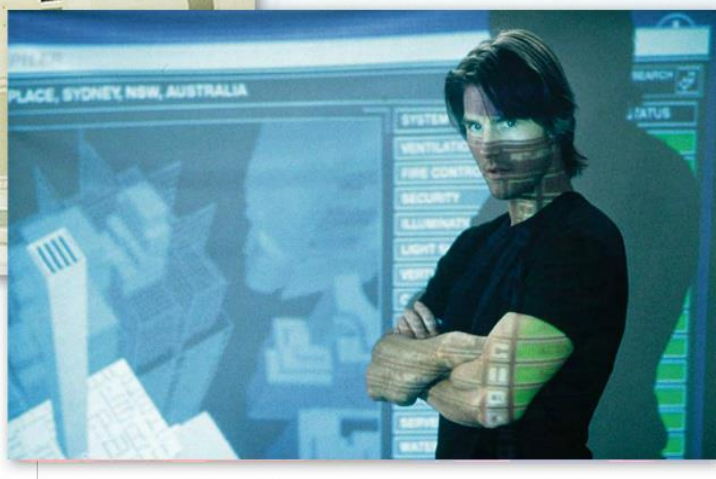
【消費宣導】
消費者保護宣導-愛美也要顧健康！疾管署呼籲民眾施打美容針應慎選合法醫療院所，以免危害健康

淺談資通安全最弱環節

◆ 臺北中正高中資訊組長 — 李詩婷

資通安全的整體安全強度，取決於系統中最弱環節，而政府機關及企業組織中，「人」往往是最容易造成資安事件的原因。

(接續次頁)



在「不可能的任務」電影中，阿湯哥飾演的伊森韓特（Ethan Hunt），出任務前會分析目標地點之建築結構、門禁及警衛編制，以從中找出最容易侵入之弱點。這種原理不難明白，即是分析對方弱點，以提高成功侵入的機會。對比資安防護，亦取決於系統中的最弱環節，而「人」就是最易侵入的關鍵點。（Photo Credit: Paramount Pictures）

最弱環節　最易被入侵

在「不可能的任務」電影中，阿湯哥飾演的伊森韓特（Ethan Hunt）往往會因任務需求，不得不祕密入侵高度防備的企業組織或政府機關，而作為一個正派特務，絕不會拿猛烈火力來硬碰硬，因此，小組人員就會開始進行行前戰略會議，包含研究分析建築物架構、門禁及警衛編制、內部員工組織分布等所有可能的入侵管道，以從中找出一絲一毫的入侵機會。這種原理不難明白，即是分析對方最容易侵入之弱點，以提高成功的機會。

「人」是資安的最弱環節

近年重大資安事件層出不窮，政府機關及企業組織無不聞駭色變，紛紛提高了資安防護的經費與人力以對抗駭客入侵。但在資通安全領域有一句名言，「資通安全的整體安全強度，取決於系統中最弱環節（Weakest Link）」，而「人」就是被公認為是這裡所指的最弱環節，從日益猖獗的網絡釣魚詐騙似乎也印證了此一論點，不管是臉書、LINE，或是簡訊，總是有推陳出新的新詐騙內容。

假冒銀行發送簡訊 客戶損失數百萬元

以近期的新聞事件為例，110 年 1 月底，駭客偽冒國泰世華網銀發送釣魚簡訊，

(接續次頁)

國泰世華銀行已在官網及 APP 上宣導相關資訊，強調「銀行不會主動要求用戶登入網路銀行來綁定用戶資料」。（圖片來源：國泰世華官方網站 https://www.cathaybk.com.tw/cathaybk/personal/news/announcement/2021/012801announceinfo；https://www.cathaybk.com.tw/cathaybk/campaign/ebanking/2021fraud）

內容為：「您的銀行帳戶顯示異常，請立即登入綁定用戶資料，否則帳戶將凍結使用」，訊息下方同時附上銀行網址要求民眾登入網路銀行。許多人驚見此訊息，心急立即點進此連結網站，而不幸被竊取其用戶代號及密碼，已有多位國泰世華網銀用戶上當；帳戶內資金被盜轉出去，短短 3 天內就有 21 人被害，損失金額高達 3 百萬元。對此，國泰世華銀行已在官網及 APP 上宣導相關資訊並暫時關閉 APP 部分功能，並強調「銀行不會主動要求用戶登入網路銀行來綁定用戶資料」。

網路釣魚常見手法

通常駭客若要成功進行網路釣魚，首先必須精心偽裝連結網址，常用手法如將字母「i」改以數字「1」取代，或是字母「w」改以連續兩個「vv」取代等方式，而此次國泰世華詐騙案所使用的偽裝手法就是將真實網址「www.cathaybk.com」改為「www.cathay-bk.com」，由於網址名稱太過接近，難怪用戶難以察覺，點了連結後當然就會被導向偽裝的惡意網站。

(接續次頁)

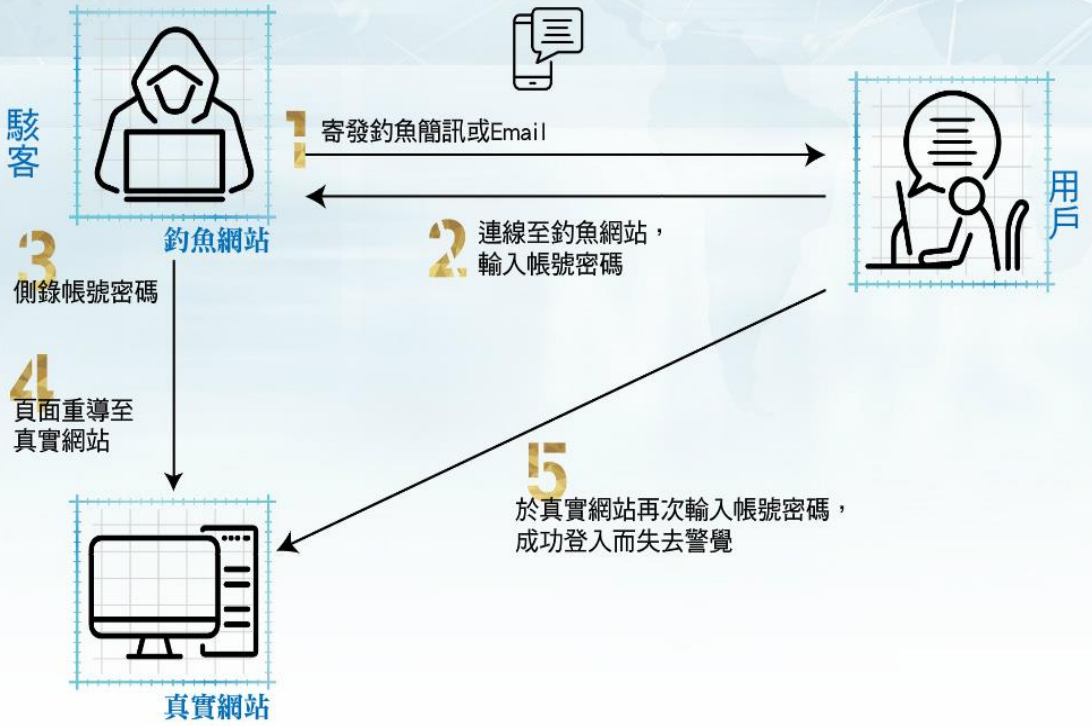


圖 1　釣魚網站非法獲取資料流程

駭客誘騙用戶點擊網址連結只是第一步，第二步則是要騙取用戶之帳號密碼，所以這時就必須利用事先架設的釣魚網站，且其網頁頁面必須跟真實網頁十分近似，包含標題、圖片及登入介面等皆需高度雷同，才能讓用戶放心點選。由於釣魚網站製作無法與真實網站完全相符，因此此時若用戶留心的話，會發現釣魚網站上的部分按鈕或連結功能可能無法點選或使用，或是輸入帳號密碼後卻沒有任何反應。更有甚者，為了不讓用戶察覺到此為釣魚網站，過往案例顯示，駭客可能在用戶輸入帳號密碼後，立即將頁面導向至真實網站的登入頁面，讓用戶誤以為是自己輸入錯誤所導致，而當用戶再次輸入帳號密碼並成功登入真實網站後，就不會察覺到第一次所輸入的帳號密碼，其實早已被駭客盜錄下來。

防範網路釣魚之自救方式

若民眾收到任何要求登入網路銀行的通知，建議可先與銀行確認，切勿直接在簡訊上點擊連結。另為避免不小心點擊到來歷不明的網址，建議民眾可以養成記住常用銀行網址的習慣，或將銀行網址加入瀏覽器書籤，**另外也可利用搜尋引擎找到正確網站，以減少被釣魚網站詐騙的風險。**

一旦懷疑自己可能已經中招，除儘速確認帳戶狀態外，另外應該趕快變更密碼，

(接續次頁)

表 1　2021 農曆年前偽冒臺灣金融機關釣魚簡訊及網站情形

日期	內容	追查釣魚網站數目	受害情況
2021/1/6	**釣魚郵件、釣魚網站** 疑似偽冒中華郵政寄送郵件，竊取個資。	1 個	不確定
2021/1/27	**釣魚簡訊、釣魚網站** 【國泰世華】您的銀行帳戶顯示異常，請立即登入綁定用戶資料，否則帳戶將凍結使用。	6 個	據警方 2 月 6 日統計，已接獲 89 件通報，25 件被害人帳戶已遭盜用，損失金額高達 518 萬元。
2021/2/5	**釣魚簡訊、釣魚網站** 【台新銀行】您好，由於網路銀行版本更新，請於 2 月 6 日前登入進行驗證，否則將停用您的使用權限，超時請至臨櫃辦理。	17 個	據警方 2 月 6 日統計，已接獲 10 件通報，7 件被害人帳戶已遭盜用，損失金額高達 55 萬元。
2021/2/9	**釣魚網站** 疑似偽冒富邦人壽官方網站，竊取個資。	1 個	不確定
2021/2/9	**釣魚簡訊、釣魚網站** 【中國信託】你的網路銀行更新失敗，請立即輸入你的驗證碼以更新資料，超時請重新輸入。	11 個	據警方 2 月 9 日統計，已接獲 1 件通報，尚未有受害者報案。

資料來源：iThome，https://www.ithome.com.tw/news/142711。

以搶在駭客前保護好帳戶資金。另外，若自己曾在多個不同網路服務中使用同一組帳號密碼，例如網路銀行、個人信箱、社群媒體及購物網站等，也必須一併更換，以避免駭客利用所竊取到之帳密資料進行多方嘗試。

為防止釣魚訊息持續橫行，各大銀行彼此串聯，共同於今年農曆春節前在各自的臉書上張貼有趣的防詐騙文案，提醒民眾詐騙集團全年無休，要隨時防範。（資料來源：國泰世華臉書粉絲專頁，https://zh-tw.facebook.com/cathayunitedbank/photos/a.160335250820488/1811446399042690）

資安防護無假期　提高警覺最要緊

網路釣魚或網路詐騙，除了針對個人進行資金詐騙外，駭客在入侵機關及企業組織時，也常選擇從機關及企業組織資安防護的最弱環節下手—即人心，利用釣魚信件或簡訊等方式為攻擊發起點，對員工進行詐騙，如此可避免直接與防火牆等資安防護設備硬碰硬，提高攻擊效率。儘管目前市面上存在惡意網址檢測及惡意郵件過濾等資安產品防護功能，但駭客釣魚手法也在進化，因此，有效培養員工的警覺心、強化資安意識及定期教育訓練，才是守護資安之最佳對策。

資料來源：清流雙月刊

國安局退訓男PO文洩密 檢起訴求重刑

台北地檢署昨依違反國家情報工作法將男子何牧珉起訴，考量他犯後態度不佳且耗費司法資源，建請法院從重量刑。（記者錢利忠攝）

犯後態度不佳 意圖耗費司法資源

擁有台大文憑的男子何牧珉，三年前考進國家安全局，在受訓時表現欠佳而被退訓，他自認遭長官刁難，竟在網路PTT論壇網站揭露同梯受訓同學及長官的職稱、化名與真實身分，導致情報人員面臨身分曝光的風險；台北地檢署認定他犯後態度不佳且意圖耗費司法資源，昨依違反國家情報工作法將他起訴，最輕刑度七年起跳，檢方並建請法院從重量刑。

(接續次頁)

到案全程緘默 反制偵查

今年八月，檢調拘提何男到案，他全程行使緘默權，檢方一度聲押，他則向法院聲請提審反制，試圖阻礙檢方的偵查程序，法院裁定八萬元交保。

檢方調查，何男畢業於台大化工系，二〇一八年考進國安局，受訓時因表現不及格，且動輒鑽體制漏洞，不到半年就被退訓。隔年十月九日、十月十二日，何男兩度在PTT貼文揭露同梯受訓同學、國安局訓練中心少校隊長、主任等人的身分與職稱，將情報人員身分曝光。

情報人員身分 故意揭露

北檢認為何男明知應永久保密情報人員的身分，卻故意上網揭露，涉犯本刑七年以上的情工法重罪，考量他兩次貼文的犯意各別，建請法院分論併罰。

與何男同梯的周姓女學員，也因遭退訓而在PTT揭露國安局官員個資，今年二月由士林地檢署起訴。

資料來源：自由時報〔記者錢利忠／台北報導〕

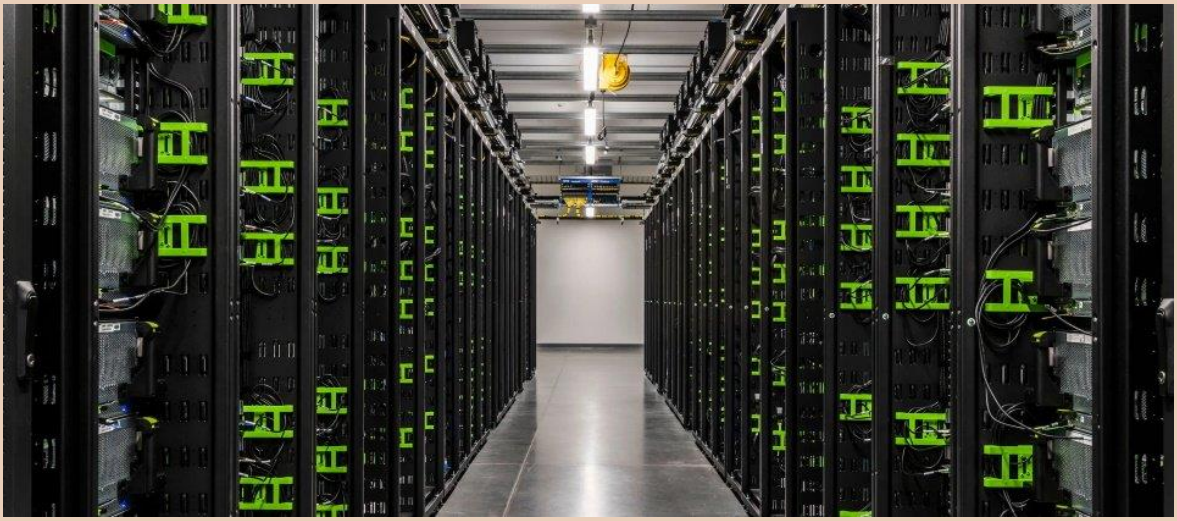
臉書公布大當機始末報告：日常維護出錯所引發的骨牌效應

在臺北時間10月5日清晨，臉書發生了這幾年最嚴重的當機事件，全球的臉書服務在同一時間斷線，涵蓋Facebook、Instagram與WhatsApp，影響全球逾35億用戶，且持續近7小時，負責工程與基礎架構的臉書副總裁Santosh Janardhan隨後公布了詳細的肇事原因，而一切都是從例行性維護出錯所引發的骨牌效應。

Janardhan解釋，這次的故障是由一個管理臉書全球骨幹網路能力的系統引起的。臉書透過骨幹網路來連結所有的運算設備，它是由橫跨全球之數十萬英里長的光纖網路所組成，負責連結臉書的所有資料中心。

臉書的資料中心有著不同的形式，有些是安置數百萬臺機器的建築物，這些機器用來存放資料，以及負責執行讓臉書平臺得以運作的運算任務，有些資料中心則是相對小型的設施，以將臉書的骨幹網路連至全球網路及使用者。

因此，當使用者開啟任一臉書家族的應用時，該應用程式會向最近的臉書設施請求資料，再藉由骨幹網路傳送到大型資料中心，而這些資料流量的傳遞即是由路由器管理。



(接續次頁)

可想而知，臉書工程師的日常任務之一就是維護此一基礎架構，而且經常要把骨幹網路的一小部份移出網路，以修護光纖、新增能力，或者是更新路由器韌體。

在5日凌晨時，臉書工程師展開了例行性維護，發布了一個命令來評估全球骨幹網路能力的可得性，卻不小心切斷了骨幹網路的所有連結，等於是讓臉書全球的資料中心同時斷網。其實臉書的系統具備稽核命令的功能，以預防類似的錯誤命令，但稽核工具中的臭蟲卻讓它沒能阻止此一錯誤命令。

接下來就發生了Cloudflare看到的事情了。Janardhan指出，雖然臉書的骨幹網路斷了，但它們的DNS伺服器還是正常運作的，相關伺服器負責回應DNS查詢，也負責透過邊界閘道協定（Border Gateway Protocol）向全球網路宣告自己的存在。

然而，為了確保可靠的運作，臉書的DNS伺服器有一項設定，就是當它無法連結臉書的資料中心時，就會關閉BGP的宣告，於是，不管是Cloudflare的1.1.1.1、Google的8.8.8.8或是其它公共的DNS解析器，都無法在網路上發現Facebook、Instagram或WhatsApp的蹤跡。

(接續次頁)

Janardhan說，一切都發生的太快了，且工程師在查明原因時又遇到了兩項障礙：一是因為網路都斷了而無法使用日常工具來存取資料中心，二是喪失了DNS也讓原本用來調查及解決故障的內部工具失效。

於是臉書只好派出工程師到資料中心，企圖手動解決問題並重啟系統，但資料中心不管是實體或系統都嵌入了安全機制，一來不容易進入，二來就算進入了，其硬體與路由器原本的設計就提高了變更的門檻，因此又花了一點時間來啟用安全存取規則，以讓這些　工程師能夠修改資料中心裡的伺服器。

在臉書成功恢復骨幹網路之後，另一個關鍵則是重啟資料中心，瞬間重啟所有服務可能會因流量與電力使用的驟增，而讓系統再度崩潰。但臉書之前即曾進行多次的「風暴」（Storm）演習，模擬系統故障的場景，關閉服務、資料中心或整個區域的系統來進行壓力測試，有了這些演習經驗，讓臉書在回復所有服務的環節上沒有遭遇太多的問題。

在處理這個意外的時候，Janardhan也察覺了一件事，過去臉書不斷地強化系統來防止未經授權的存取，但這些機制卻也拖慢了臉書自己修復的腳步，即便如此，他依然相信這個取捨是值得的。

資料來源：ITHOME電週文化事業

涉洩密給殯葬業，11警消遭訴！

新北市警察局和消防局勤務中心人員，涉嫌收取殯葬業者佣金，讓業者搶先得知訊息以便承接業務。檢方今天起訴11人。

起訴書指出，殯葬業者為避免爭搶意外案件產生糾紛，彼此在10多年前共同協議以「先到先贏」作為遊戲規則，一直延續至今。吳姓和林姓男子，合資成立禮儀公司，為了搶時間，透過親戚和舊識，以協助調職、參加聚餐等方式，搭上新北市警局和消防局勤務中心人員。

檢方指出，吳男和林男涉嫌向值勤員表達若接獲意外死亡或自殺通報，可透過電話私下告知事發地點，業者再派員趕赴現場，或轉給其他配合的禮儀公司，如果順利承接，將提供新台幣1萬元到2萬元不等的佣金。

新北地檢署在民國101年4月12日指揮台北市調查處，兵分2路前往吳男及林男位於新北市三重區及板橋區住居處搜索，當場查扣大筆帳冊及亡者名單，經清查後，將7名當時任職110及4名119勤務中心人員，依涉犯「貪污治罪條例」移送地檢署偵辦。

檢方認為，被告等人有受理民眾報案，並有向上級陳報及通知的職權，雖私下告知殯葬業者，但因不屬於職權範圍內的事項，難以認定涉犯貪污治罪條例的「職務上的行為」。

但檢方表示，相驗往往是檢察官開始偵查的原因，相關人員接獲通報後，應依循「偵查不公開」原則，依刑法第132條「洩漏國防以外應秘密罪」，起訴11人。

與惡的距離

壹、案例故事

印尼籍春嬌和越南籍志明在臺北火車站因假日活動而認識，漸漸日久生情互有好感而成為一對戀人，在友情昇華成愛情且後，志明決定與春嬌在臺灣長相思守。無奈為了應付春嬌的日常龐大花費，竟然挺而走險行搶而被警察逮捕送進看守所。沒想到衰事接連而來，愛人春嬌竟然劈腿菲律賓籍麥克而跟志明分手，志明化悲憤為力量，立誓要學好英文，希望能從此跳脫「黑手」的低薪工作。為了聽懂CNN新聞和TIME雜誌，志明在看守所期間，向管理人員提出要購買收音機及閱讀報紙的請求，管理人員小箭卻告知志明，因為他目前仍在禁見中，因此不得購買收音機、電視機或閱讀報紙，故拒絕他的申請。然而志明仍不放棄，持續向機關反映，希望修改此不合人道的規定，主張收押禁見者仍應享有獲得知識的權利，以吸收資訊，減少因時間過長，導致無法重返社會的結果。

貳、爭點

禁止接見者不得禁止使用收音機、電視機或閱讀報紙，是否不人道且侵害其人性尊嚴？

參、人權指標

一. 《公民與政治權利國際公約》第7條規定：任何人不得施以殘酷，或予以殘忍、不人道或侮辱之處遇或懲罰。非經本人自願同意，尤不得對任何人作醫學或科學試驗。

二. 《公民與政治權利國際公約》第10條規定：自由被剝奪之人，應受合於人道及尊重其天賦人格尊嚴之處遇。

(接續次頁)

肆、國家義務

一. 國家對待自由受剝奪者，應如同自由的人一樣，必須保障這些人的尊嚴及得到基本的尊重，而且不得使其遭受與剝奪自由以外的任何困難或限制。喪失自由者，除了在封閉環境中，不可避免須受的限制外，享有《公政公約》規定的所有權利（人權事務委員會第21號一般性意見第3段意旨）。

二. 刑事訴訟法第105條第3項及第4項規定，關於禁止被告接見、通信及受授物件等事務，偵查中由檢個案有特別限制不得被告閱讀報紙、收看電視及收聽廣播外，禁見被告仍可以主張閱讀報紙、收看電視及收聽廣播。

伍、解析

一. 司法院大法官釋字第653號解釋，刑事被告受羈押後，為達成羈押之目的及維持羈押處所秩序之必要，其人身自由及因人身自由受限制而影響之其他憲法所保障之權利，固然因而依法受有限制，惟於此範圍之外，基於無罪推定原則，受羈押被告之憲法權利之保障與一般人民所得享有者，原則上並無不同。有鑑於此，過往相關規定未符合該原則應予以修正。

二. 對於禁見被告禁止使用收音機、電視機或閱讀報紙之規定，係按照臺灣高等檢察署86年1月4日檢仁所甲字第17號函示規定辦理，其限制目的，係為避免共犯或相關利害關係人等，利用電視、廣播等傳播媒體，或以公開報導、刊登廣告等方式，藉此傳遞串（證）之相關訊息，然而禁止措施雖為達成羈押目的，然恐與比例原則未盡相符，且已不符人權趨勢及時宜。

三. 法務部矯正署經檢討後，業於107年2月9日通函矯正署所屬各矯正機關，臺灣高等檢察署86年1月4日檢仁所甲字第17號函示停止適用，對於原禁見被告之接見、通信及受授物件等事務，不再完全禁止，而須視個案而定。

四. 本案例中，禁見中的志明，除非法官或檢察官有特別囑咐不得讓他閱讀報紙、收看電視及收聽廣播外，志明仍然可以請求購買收音機、電視機或閱讀報紙，管理人員小箭也不得因此拒絕，否則有違《公政公約》第7條及第10條不人道處遇之規定。

資料來源：內政部移民署108年人權教材

愛美也要顧健康！疾管署呼籲民眾施打美容針應慎選合法醫療院所，以免危害健康

愛美雖是人的天性，但在進行醫美療程前，仍應充分瞭解相關資訊，以免危害自身健康。疾病管制署公布國內今（2018）年首起民眾疑似因施打美容針引發肉毒桿菌中毒案例，居住北部的40餘歲女性，曾於國外非醫療機構之美容中心施打不明成分美容針，施打4天後開始出現吞嚥困難、視力模糊及呼吸費力等症狀，至某醫學中心就醫並說明曾赴國外注射疑似肉毒桿菌毒素，經醫師評估後通報疑似肉毒桿菌中毒與採檢。由於個案通報採檢時間距注射肉毒桿菌毒素時間已超過3週，檢驗結果為陰性，但依其症狀及流行病學資料研判，應屬極可能病例。

國外文獻和新聞稿指出，香港2016年5月接獲首例疑似在注射後發生肉毒桿菌中毒之個案通報，截至2018年11月累積17例通報疑似個案，其中11例曾到中國大陸接受注射。另中國大陸一篇文獻彙整2009年4月至2013年6月共有86例醫源性肉毒桿菌中毒個案，為現有文獻中累積個案數最多者。埃及於2017年6至7月期間發生9人因注射未經許可之肉毒桿菌毒素仿冒品之後出現中毒現象。

(接續次頁)

疾管署表示，肉毒桿菌中毒的傳染途徑可分為：（1）食因型（又稱傳統型）：食用遭肉毒桿菌毒素污染的食物造成，大部分的肉毒桿菌中毒屬此類；（2）腸道型：常發生於腸內免疫系統缺損或腸道菌叢未健全的人，食入肉毒桿菌孢子增殖後產生毒素而引起；（3）創傷型：傷口深處受到肉毒桿菌孢子污染產生毒素導致中毒，常與藥物濫用有關；（4）醫源性：注射肉毒桿菌毒素，如醫學美容等人為因素導致之中毒。

疾管署進一步指出，醫源性肉毒桿菌中毒，可能於注射肉毒桿菌毒素後數小時、數日或數週發病，症狀包括腹瀉、腹痛、便秘、食慾不振、嘔吐、倦怠、眩暈、昏睡、複視、眼瞼下垂、瞳孔放大或無光反射、顏面神經麻痺、講話困難、吞嚥困難、失去頭部控制能力、肌肉張力低下及全身性虛弱等，並可能發展為呼吸無力衰竭，甚至死亡。如出現疑似肉毒桿菌中毒症狀，須及時前往醫療院所診治。醫師除採取相關治療措施外，應進行法定傳染病通報
。

疾管署呼籲，接受不當的肉毒桿菌毒素注射，可能對健康造成威脅，民眾在接受肉毒桿菌毒素等醫學美容療程前，應瞭解相關醫療資訊，如：確認該機構為立案登記醫療院所、肉毒桿菌毒素注射執行者為合格醫事執業登記之醫事人員、醫師能提供諮詢注射後可能出現副作用或併發症處理、主動詢問注射製劑成分及是否有藥品許可證字號等資訊，以降低可能潛在的風險。民眾如有相關疑問，可參考疾管署全球資訊網（https://www.cdc.gov.tw）「肉毒桿菌中毒Q&A」，或撥打免付費防疫專線1922（或0800-001922）洽詢。

資料來源：衛生福利部疾病管制署網站

國民年滿18歲
有公民投票權

投票時間：110年12月18日・上午8點至下午4點

公投12.18 人民是投家

請禮讓行動不便、乘坐輪椅、孕婦及年長者，優先進入投票所投票。

中央選舉委員會
Central Election Commission

廣告

投票帶3寶

國民身分證·投票通知單·印章

投票時間:110年12月18日・上午8點至下午4點

公投12.18 人民是投家

投票時請戴口罩。請勿使用印章或指印圈選，以免形成無效票。

中央選舉委員會
Central Election Commission

8月9日(含當日)後戶籍遷出者
須返原戶籍地投票

投票時間:110年12月18日・上午8點至下午4點

公投12.18 人民是投家

中央選舉委員會
Central Election Commission

廣告

8月9日後遷籍者公投看過來！

1. 「110年全國性公民投票」受疫情影響，原定8月28日投票，改定於12月18日舉行。

2. 仍以原投票日有投票權為限。

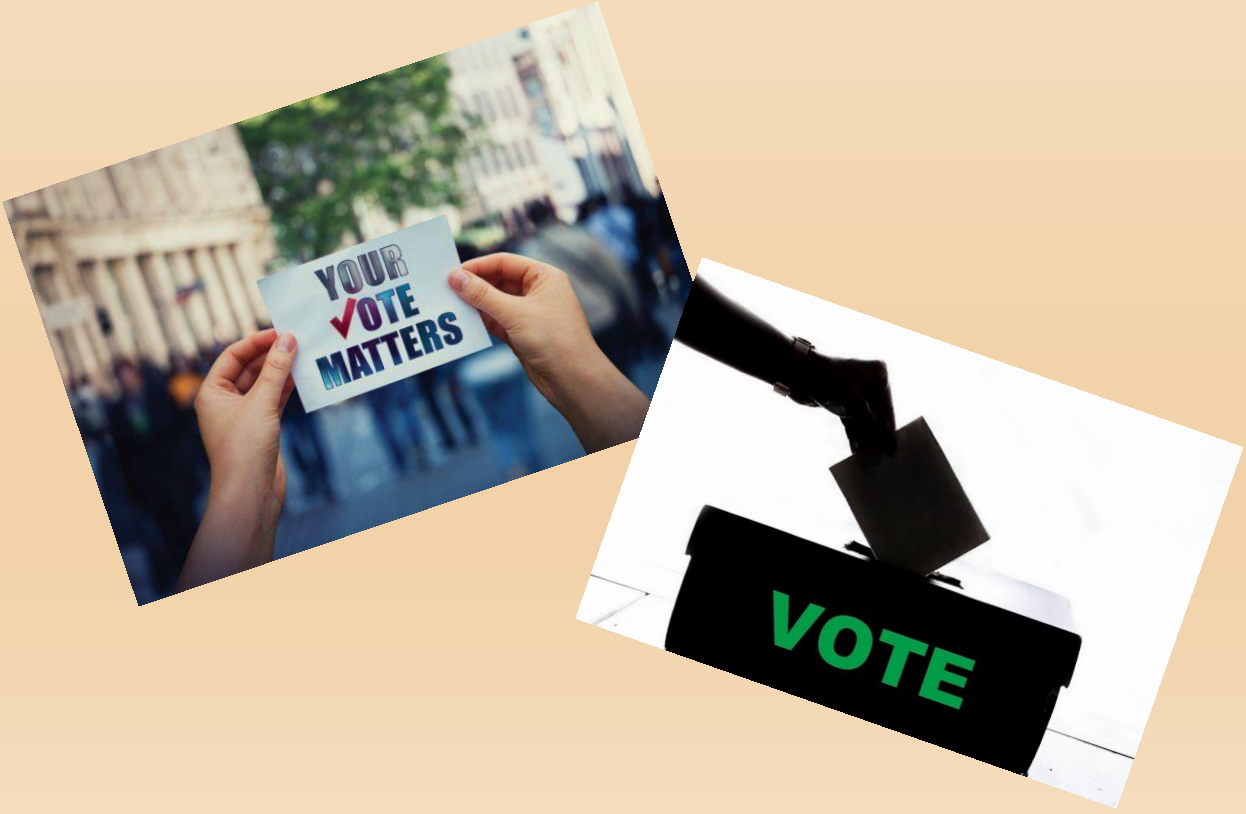
3. 依公投法第24條準用公職人員選舉罷免法第20條，已編入名冊之投票權人，於110年8月9日（含當日）後遷出者，應在原戶籍地投票所投票。

公投12.18 人民是投家

投票時間：110年12月18日・上午8點至下午4點

中央選舉委員會 Central Election Commission

廣告

政風電子報

刊名 / 政風電子報
出版機關 / 內政部移民署政風室
地址 / 10066臺北市中正區廣州街15號7F
出版年時間 / 中華民國110年11月
頻率 / 月刊
編輯總召 /卓明偉
主編 / 簡國樑
本室編輯小組 / 張文山、陳安莉、蘇承玉、
陳怡安、蔡雅雯、謝瑋哲