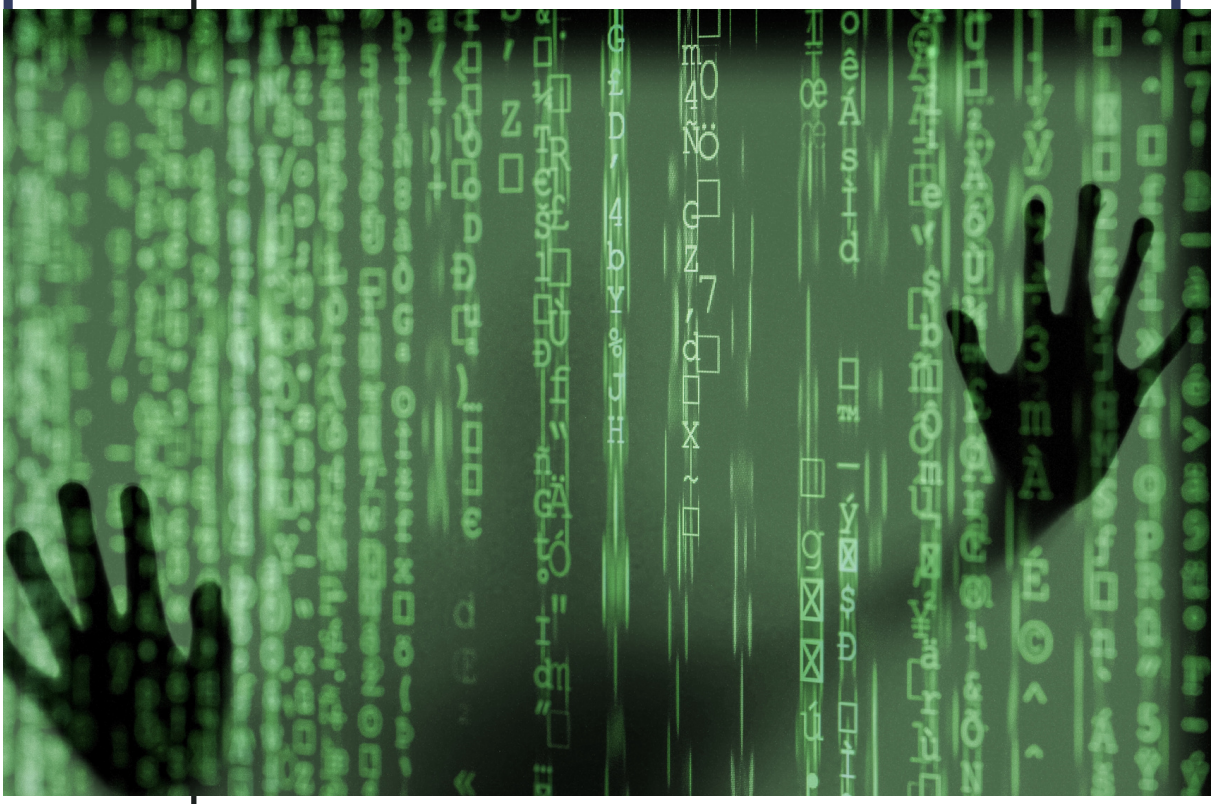
公務機密
資訊安全維護



網路犯罪要小心，四招資安習慣保護你

以下提供四個小撇布:

1.點擊連結前先確認
2.下載APP時多確認
3.密碼強效長更新
4.資安事件要通報

農業部林業及自然保育署臺東分署

公務機密 資訊安全維護

目錄

華郵：解放軍駭入日本機密軍事網絡 狀況嚴峻

2023-08-08 09:39 聯合報／ 記者張文馨／華盛頓即時報導

華盛頓郵報7日獨家報導，美國國家安全局2020年秋天發現，解放軍駭入日本機密的軍事網絡，持續竊取計畫、能力、軍力缺陷評估等資料；川普和拜登政府的副國安顧問分別飛往東京示警，美國前軍事官員稱狀況非常嚴峻。

美日正著手強化網路安全，但報導並未提到狀況是否已經排除。

中國大陸駭客駭入美國商務部長雷蒙多（Gina Raimondo）、美國國務院亞太助卿康達（Daniel Kritenbrink）和美國駐北京大使伯恩斯（Nicholas Burns）的電郵，竊取美國內部對中政策的討論與評估，全案還在調查中。

華盛頓郵報引述十多名美日現任與前任官員來說明這項未曾曝光的發現，美國國安局2020年秋天發現解放軍對日本的行動，時任美國國安局局長暨網路司令部負責人中曾根（Paul Nakasone）與白宮副國家安全顧問博明（Matthew Pottinger）趕往日本東京，對日本防衛大臣簡報，並透過防衛大臣安排，直接對日本首相示警。

根據報導，美方告訴日本政府，北京已經突破東京的防衛網絡，這是日本近代以來最嚴重的駭客攻擊之一；日本方面大感意外，但表示會調查此事。

不過華府當時面臨選舉無效之爭和政權交接，雖將這件事情列入政權交接事項，但重視程度不足，拜登政府上台後，開始在美國監督下強化日本網路安全，包含美方派人赴日協助東京研判被駭範圍，著手清理潛藏的中國大陸惡意軟體，以及強化網路安全的建議。

報導提到，和其他主權國家一樣，日本對於美國協助調查並建議強化其軍事網絡安全一事非常謹慎；由於美日沒有共同應對敏感情報威脅的經驗，美國要求日本提升美方在日本網路的訪問權限，日本多有疑慮。

在調查過程中，雙方達成共識，日本委託國內企業抓漏，再由美方國安會和網路司令部組成的小組檢視評估成果，並提供改善建議。

此外，白宮國安會與日本國家安全保障會議，以及美日國防部會的官員分別籌組對話機制，定期交換訊息；2021年秋天，美國再次發現中國大陸侵犯日本防衛系統的訊號。

副國安顧問紐柏格（Anne Neuberger）在2021年11月率一眾官員在日本疫情封閉國門之際，飛往東京會晤日方軍事、情報與外交高層官員示警，並向日本強調此事必須解決。

2022年12月，時任白宮國家網路主管英格利斯（Chris Inglis）訪日，與日本政府分享美國如何保障網路安全；美國今年3月也發布了國家網路安全戰略。

在兩國合作強化網路安全部分，日本成立24小時監控的網路司令部，建立持續分析軍用電腦系統風險的計畫，強化網路安全訓練並計畫5年內花費70億元用於網路安全，防衛省的網路安全人力擴張到4000人。

華盛頓郵報報導，東京已經採取步驟強化網路安全，但研判這樣仍不足以抵擋北京的駭客攻勢；而這點可能影響美日的情報共享。

美國資深官員對華盛頓郵報表示，美國一直在關注中方間諜行動，同時北京一直在發展網路攻擊能力，以便用來切斷美國與亞洲重要盟友的關鍵服務，在危機或衝突發生時影響決策。

一名美國資深國防官員表示，日本正大量投資推動強化網路安全，但工作有待完成，網路安全之於美日聯合行動至關重要，美日聯合行動更是美日聯盟的核心。

近3成外館有資安疑慮 數位部：使用中國產品須造冊列管

〔記者徐子苓／台北報導〕去年有近3成駐外館處採用有資安疑慮的設備或服務，數位部今（4日）表示，有些外館因為當地市場關係，不得已只能使用中國製資通產品，這些產品都會經過外交部資安長核准、造冊列管，數位部也會親自到外館強化資安健檢，目前並沒有發現重大資安事件。

審計部111年度中央政府總決算審核報告揭露，外交部截至去年底111個駐外館處中，有31個使用有資安疑慮的設備或服務，不合格率近3成。報告指出，外交部因業務屬性機敏，常為駭客攻擊目標，且駐外館處受限駐地環境非由我方掌控，加上駐外人員資訊技術能力相對不足等，恐成整體資安防護缺口。

事實上，針對公部門資安，數位發展部定期調整「危害國家資通安全」的產品清單，其中包含許多中國製的資通訊產品，依法禁止公務設備使用。

數位部次長李懷仁今天出席活動時受訪解釋，「危害國家資通安全」產品，公部門並非都不能使用，而是原則上禁用；但若有必要使用，必須簽報資安長核准、造冊列管。

李懷仁說，有些外館確實因為當地市場的關係，只能使用中國製產品，意即當地產業提供的資通訊產品只有中國製，這時就要依規範簽報外交部資安長核准，造冊列管，並且強化資安檢查；這部分數位部也有和外交部保持密切聯繫，目前並沒有發現重大資安事件。

李懷仁強調，數位部有協助、參與外交部的資安健檢，其中外館涉及很多機敏資料，是由外交部主導，而數位部和國安單位都會去參加資安健檢，數位部也有同仁會親自飛到當地外館協助檢查。

外交部截至去年底111個駐外館處中，有31個使用有資安疑慮的設備或服務。（資料照）

120筆民眾個資外洩 警方一查禍首竟是自己人……

〔記者吳政峰／台北報導〕台北市警局2020年間發現一名徵信業者竟有120筆民眾個資，經查外洩源頭竟是一名王姓小隊長。台北地院依違反個人資料保護法等罪，判王員2年刑，緩刑5年；懲戒法院一審去年判王員休職1年6月，二審日前維持，全案確定。

王員不滿被休職1年6月，上訴主張，一審僅以他侵害人民資訊隱私權而判決，並未考量他無犯罪所得，且已繳交50萬元公益捐，此屬足以影響懲戒輕重之事由，一審未就此說明清楚，屬於判決不備理由，當然違背法令，應予廢棄。

但二審指出，王員上訴意旨指摘一審判決違背法令，求予廢棄，並改判較輕之懲戒處分，經核均無理由，且本件並無法律問題存有疑義而須加以辯論，亦無其他另須以言詞辯明或說明的狀況，無行言詞辯論必要，合議庭日前評議後逕予駁回，全案確定。

判決指出，台北市警局2020年4月間偵辦民眾刑事案件，發現王員疑接受文山第一分局前呂姓警員（2016年7月5日退休）請託，使用警政署警政知識聯網查詢民眾個資後，透過當面告知、通訊軟體或翻拍等方式提供給呂男，再由呂提供給徵信業者，涉嫌違反個人資料保護法及犯刑法洩密等罪，立刻報請台北地檢署檢察官指揮偵辦。

北檢去年11月16日指揮北市警政風室，及警政署政風室對王員等人執行搜索調查，複訊後認王員犯罪嫌疑重大，有湮滅、偽變造證據或勾串共犯或證人之虞，2021年11月17日向北院聲請羈押禁見獲准，2021年12月8日被北市府核布停職令，直到2022年1月11日北院裁定以20萬元交保後，3月1日才核定復職。

北檢4月11日偵查終結，依違反個人資料保護法等案件提起公訴，北院7月29日認定王員觸犯120罪，每罪各處1年2月刑，應執行2年刑，緩刑5年確定。

北市府審酌王員違法行為，已違反公務員懲戒法規定，嚴重傷害國家公務員形象，侵犯人民資訊隱私權，使人民喪失對國家信賴，決議移請懲戒法院審理。

懲戒法院一審表示，王員僅因受昔日警校同窗請託，竟多次濫用國家賦予權限，恣意查詢並洩漏個人資料，破壞政府機關形象，足使民眾喪失對公務員執行職務的尊重及信賴，為維護公務紀律，有懲戒必要。

一審指出，王員受託查詢民眾個人資料達120筆，侵害個人隱私，危害公務機關對於資訊管理正確性，並嚴重損害公務員形象及機關信譽，惟考量其於刑事案件偵審中坦承違失，在職期間曾獲多次嘉獎、記功等職務表現，決議判處休職1年6月，期滿回復原職。

博客來3000會員個資外洩元兇是境外駭侵 北檢簽結

刑事局持續會同數位發展部等主管機關對電商業者進行資安訪談，提供相關技術支援。（刑事局提供）

〔記者錢利忠／台北報導〕刑事局先前公布去年高風險賣場前五名，以網路書店「博客來」居首，自去年開始，警方陸續接獲書店會員報案，指才剛下單商品即收到詐騙集團來電，警方一度懷疑是內部員工外洩3000名會員個資，經檢送台北地檢署調查後，認定該平台個資外洩的原因，來自於境外駭侵，查無博客來內部人外洩個資的不法情事，已將全案簽結。

刑事局曾指出，近來在拍賣平台上賣東西的個人賣家遭詐案件，有逐步增加的趨勢，詐騙手法先由歹徒假冒買家，透過拍賣平台聊天系統，以「無法下單」名義，傳送假的拍賣平台客服連結或QR CODE給賣方，再假冒客服以「賣家未認證或簽署金流協定」等話術，騙取民眾銀行帳戶資訊，之後另以認證或簽署等名義，要求民眾操作ATM或網路銀行，將被害款項匯出。

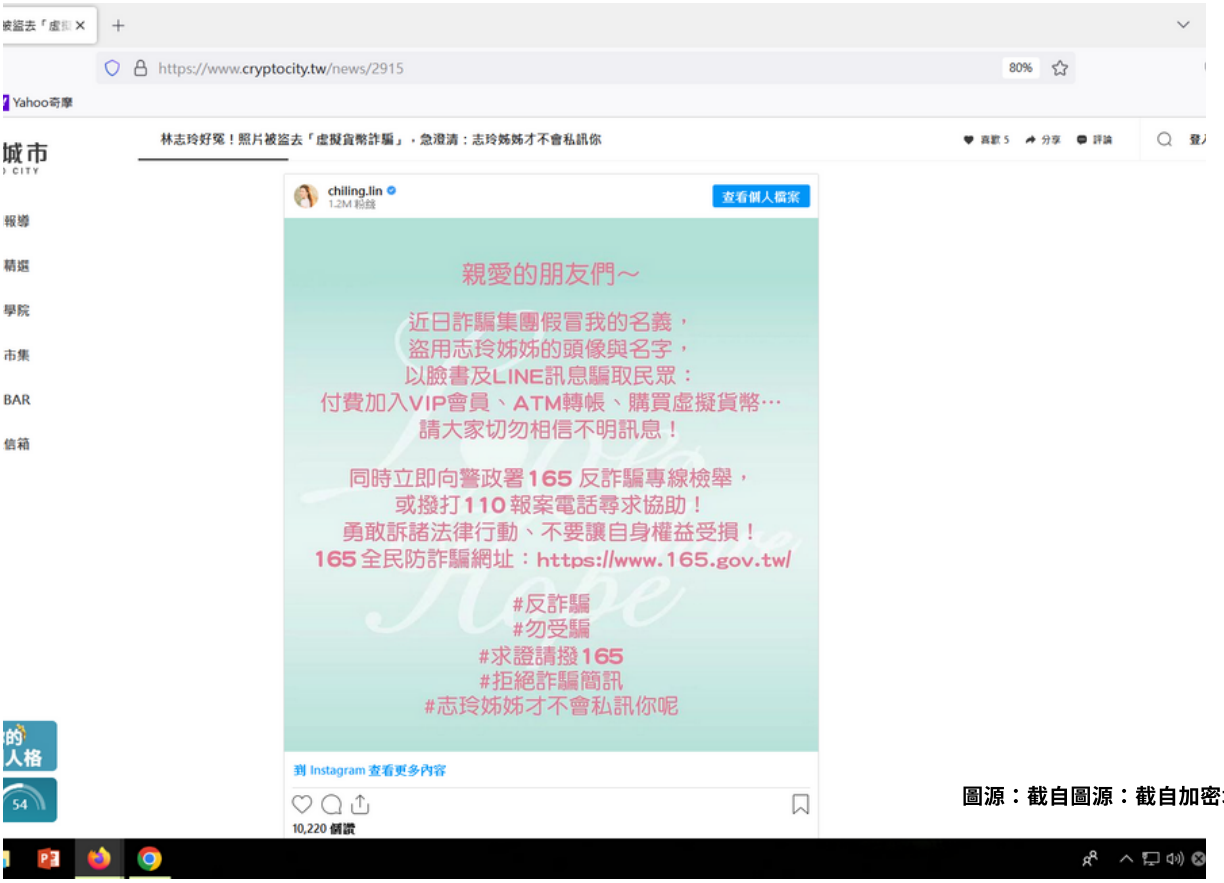
個資外洩的問題頻傳，從政府機關的健保、戶政資料，以及民間企業的華航、IRENT、博客來網路書店、誠品書店等，都發生民眾個資遭外洩情況，日前甚至有讀者在誠品書店網購書籍，事後竟接到「統戰市調」電話，引起民眾關注個資外洩議題。

現行個資法對於非公務機關（即企業）洩漏個資，主管機關須先要求「限期改正」，最高只能罰20萬元，外界認為罰則不夠重，立法院已完成修法初審，未來企業若違反安全維護義務，情節重大最高可處1500萬元，該修法仍待三讀通過。

詐團假冒林志玲騙投虛擬貨幣，本尊出面提醒

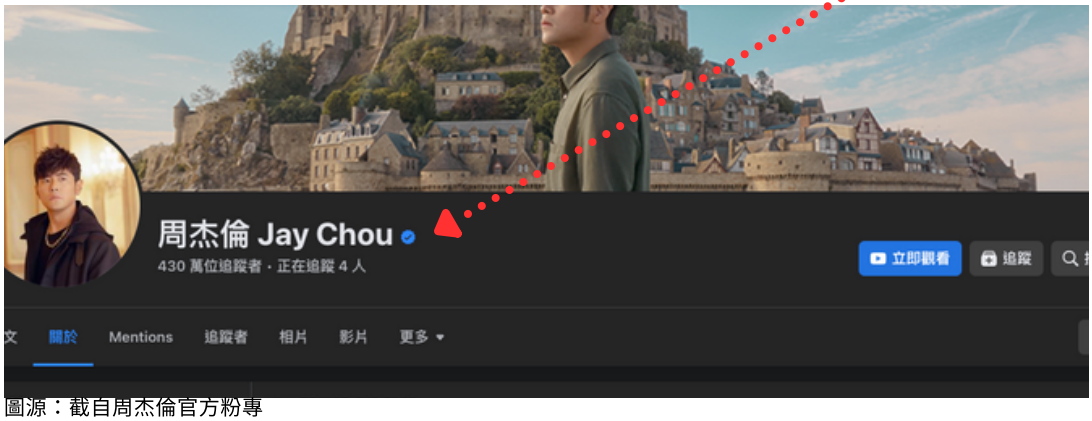
台灣詐騙集團花樣多，假冒名人騙取普通人的信任，更是常用的招數之一。
近日「台灣第一名模」林志玲突然在臉書、IG 社群發文，透露最近有詐騙集團開始假冒她的名義，在社群上誘騙民眾去購買虛擬貨幣、ATM 轉帳等。除了提醒大家不要相信不明訊息、主動撥打 165 求證外，她還在文末逗趣地強調：

「志玲姊姊才不會私訊你呢」



圖源：截自圖源：截自加密城市

在貼文下方，也有一些網友分享遇到詐騙份子的經驗。有人表示就曾收到假林志玲的訊息，企圖誘騙他賣出價值 300 美元的 STEAM 卡，並要求他加入 LINE 帳號；也有人表示曾被假冒成林志玲的日本籍丈夫私訊，對方的中文還十分流暢。
據了解，林志玲目前只擁有官方臉書、INSTAGRAM、微博（都有藍勾或金 V 驗證），並沒有所謂的官方 LINE 帳號，而她的私人 LINE 帳號更不會輕易洩漏。
因此，若遇到有人在 LINE 上聲稱自己是林志玲，就要小心詐騙。



圖源：截自周杰倫官方粉專

惡意程式CHERRYBLOS利用OCR技術竊取帳號密碼

文/林妍溱|2023-08-01發表

趨勢科技發現近期透過釣魚網站散布的CHERRYBLOS竊密程式，能以光學辨識（OCR）技術竊取受害者輸入的加密貨幣錢包憑證資料

安全廠商趨勢科技近日發現一隻ANDROID竊密程式，能利用光學辨識（OCR）技術萃取出手機螢幕的文字，以竊取帳號密碼。

趨勢科技今年4月發現二波有關的惡意程式攻擊。其中一波是透過釣魚網站散布名為CHERRYBLOS的竊密程式，另一波則是存在GOOGLE PLAY STORE上的詐騙APP。

其中CHERRYBLOS具備使用OCR圖像辨識工具的進階能力。今年4月CHERRYBLOS嵌入於挖礦軟體的APP中，透過推特、TIKTOK、TELEGRAM等傳播，廣告連結將用戶導向釣魚網站下載到其ANDROID手機上。CHERRYBLOS目的在竊取加密貨幣帳號的憑證，並在用戶提款時置換錢包網址為攻擊者所控制的網址，以掏空用戶錢包。

研究人員發現，CHERRYBLOS具有多種高明技倆以避免偵測。為躲避靜態偵測，惡意程式作者以強大的市售封裝工具JIAGUBAO（360加固保）內建加密技術封裝，以加密CHERRYBLOS大部分字串，減少被偵測的機率，也會以WEBVIEW顯示官網以免受害者起疑心。

CHERRYBLOS和金融木馬程式很像，會要求輔助功能的存取許可。它在用戶開啟電子錢包APP後顯示對話提示窗，要求使用者同意給予許可。CHERRYBLOS還會假造電子錢包APP啟用活動，以誘使用戶輸入密碼片語（PASSPHRASE）。很特別的是，取得輔助功能存取許可後，當用戶在螢幕上輸入密碼時，CHERRYBLOS會先拍下螢幕擷圖，以OCR翻譯成文字格式後，將密碼片語、連同植入的電子錢包APP套件名稱等資訊，傳送給駭客控制的C&C伺服器。此外，當用戶從交易平臺提款存到自己的線上電子錢包時，CHERRYBLOS會將錢包網址置換成攻擊者所控制的網域，以便竊取加密貨幣。

研究人員還在GOOGLE PLAY STORE上發現不含CHERRYBLOS的同樣的APP。他們相信是由同一個團隊開發。

此外，除了CHERRYBLOS外，研究人員也在GOOGLE PLAY上發現疑似和CHERRYBLOS有關的惡意APP，因其使用相同的網路基礎架構及APP憑證。這些APP謊稱用戶可經由導流量賺取獲利，但受害者最後是提不出錢的，故其中的惡意程式被研究人員稱為FAKETRADE。倒楣的用戶下載安裝這些APP後大量給予負評。

這類詐騙APP共有31款上傳GOOGLE PLAY STORE，現已全數為GOOGLE移除。

安全廠商提醒，用戶應避免從第三方網站下載不熟悉的APP。且安裝前應仔細審閱其他用戶的評論，看看是否有提及可能是惡意程式。此外也應留心APP要求的許可，特別是要求輔助功能存取權限。

圖片來源: MOHAMED NOHASSI ON UNSPLASH