公務機密
資訊安全維護

指導單位：行政院資通安全處、教育部
主辦單位：行政院國家資通安全會報技術服務中心

資安時事案例

電話通知被匡列是詐騙？6點了解疫調程序

當你個資外洩時會發生什麼事？

生活中的資安

NFT騙局以及安全建議

個人資料保護法

輕鬆看懂個人資料法

數位學習

106年資安動畫金像獎 荊科駭秦網

（示意圖/取自pixabay）

電話通知被匡列是詐騙？ 6點了解疫調程序

何渝婷 2022年1月19日

近期國內本土疫情擴散，根據中央流行疫情指揮中心公布的數據，今日新增54例COVID-19確定病例，分別為10例本土個案及44例境外移入。

隨著疫情升溫，全台持續擴大採檢。但近期在社群平台和通訊軟體流傳一則訊息，撰文者指出，他接到電話通知自己被匡列，須核對個資，所以要求他交出身份證字號、出生年月日和全名等，並表示衛生局稍晚會跟他聯絡。

該名撰文者立即打去衛生局求證，並發現是詐騙。

台灣事實查核中心向新北市衛生局、桃園市衛生局和中央流行疫情指揮中心諮詢後，分享相關疫調程序。

掌握接觸者名單

民眾若染疫，地方衛生局會先進行疫調來掌握確診者密切接觸者名單，若能掌握到的名單，衛生局疫調人員會以電話通知其進行採檢。

以電話確認接觸事實

在疫調程序上，地方衛生局會先與被匡列的對象透過電話確認「接觸事實」，像是詢問民眾是否與確診者在哪個時間、哪個地點接觸。

詢問個資

在確認完「接觸事實」後，地方衛生局將會再詢問被匡列者的姓名、電話、身分證字號、生日等資料，以利安排後續採檢，並會在電話中告知被匡列者的採檢時間和地點。

不會詢問被匡列者的問題

新北衛生局強調，疫調人員打電話給被匡列對象者時，會明確告知是衛生單位，並先確認接觸事實，後詢問個人資料，不會電話一接通就直接詢問個人資料。

另外，地方衛生局蒐集民眾個資只是為了確認身分、安排民眾採檢及登錄系統，並不會問到民眾的收入、銀行戶頭、個人帳號等財務相關資料。

如何防範詐騙

中央流行疫情指揮中心發言人莊人祥指出，若要判斷來電疫調者是否真的是衛生單位的疫調電話，可以反問三個問題，包括是在何種接觸指標的情境下被匡列為接觸者；接觸時間及地點為何；留下來電者的機關名稱、姓名及公務聯繫方式。

可回撥確認

若在接到疫調電話後仍有疑慮，民眾可以回撥衛生局的防疫專線或打到衛生局的總機來進行詢問確認。

當你個資外洩時會發生什麼事？

資料來源:趨勢科技部落格 (本文為合作企劃文章)
當您的姓名、出生年月日、照片、聯絡方式、信用卡號、銀行帳戶資料，以及用於各種網路服務認證上的帳號與密碼在網路上外洩，會發生什麼事呢？

如果這些資訊落到惡意的第三方手中，可能會發生隱私受到侵害、財物損失、被他人假冒、被跟蹤或脅迫等情況。因此，我們必須在平時就小心運用及管理自己和家人朋友的個人資料。

BBC 報導指出一個叫做「Maktub」的勒索病毒 在 2016 年大量散發網路釣魚郵件,警告收件人積欠某企業機構數百英鎊，要求他們點郵件中的連結列印發票，而這個連結會讓電腦感染勒索軟體。有些網路釣魚郵件還冒名專門輔導更生人或監獄受刑人的慈善機構。值得注意的一點是，網路釣魚（Phishing）郵件內容當中不僅寫出了收件人的姓名，還附上了受害人的地址。包含 BBC 的工作人員在內，都發現這些地址的正確性頗高。據推測這些資料很可能來自一些外洩事件中失竊的資料庫。

犯罪分子可能會拿你的個資做的八件事

1.一旦你的個人身份資訊（PII）被盜，通常會在暗網上賣給那些會將其用於惡意用途的人。它可以被用來： 破解其他使用相同帳密的帳號（透過憑據填充）。
2018年有300億次這樣的攻擊。
2.登入你的網路銀行帳號來取走資金。
3.以你的名義辦理銀行帳號/信用貸款（這可能會影響你的信用評等）。
4.以你的名義訂手機或將你的SIM卡轉到新裝置（這每月影響7,000名美國行動網路運營商Verizon客戶）。
5.以你的名義購買昂貴物品（如新手錶或電視機）用於犯罪轉賣。這通常是透過劫持你在電子零售商的網路帳號進行。據說電子商務詐騙每年大約造成約120億美元的損失。
6.提交虛假的退稅單，以你的名義收取退稅。(美國曾發生駭客蒐集民眾個資騙過了稅單申請服務的身份驗證程序，盜領退稅恐達15億的事件)
7.利用你的保險詳細資料進行醫療服務。
8.可能會入侵工作帳號來攻擊你的雇主。

如何防止資料外洩?

1.請密切注意自己的銀行帳號/信用卡是否有異常的支出活動。

2.如果你懷疑資料被濫用，請立即凍結信用。

3.使用網路服務前要三思, 不要在社群媒體上過度分享。

4.如果廠商告知你的資料可能已經外洩，請立即變更密碼。所有的帳號都使用強且唯一的長密碼

5.請記住，如果在網路上看到東西好的太不真實，那通常就是假的。

6.在外時如果沒有VPN就不要使用公共無線網路，尤其是要登入敏感網站時。

7.不要點開不請自來郵件內的連結或附件檔。

8.只從官方應用商店下載應用程式。

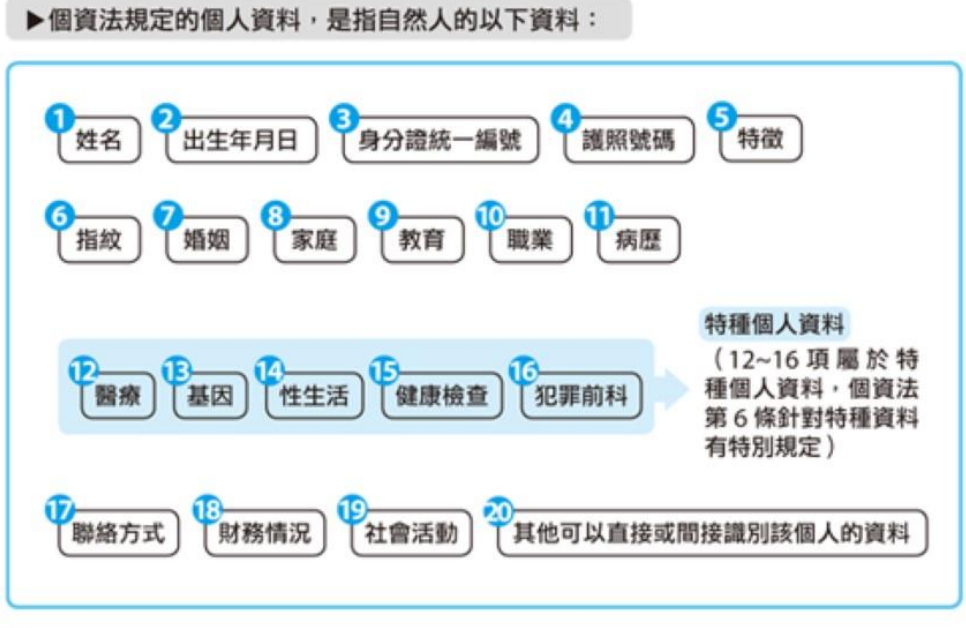
9.為所有的電腦和行動裝置安裝知名廠商的防毒軟體,如趨勢科技PC-cillin。

10.確保所有的作業系統和應用程式都保持在最新版本（即經常更新修補程式）。

輕鬆看懂個人資料法

個人資料保護法所保護的個人資料，是指自然人的姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接識別該個人的資料。

個資法所指的「個人」，是生存的自然人，因此個資法是保護自然人的個人資料，當自然人死亡後，其個人資料就不受到個資法的規範；另外，公司、法人等非自然人的資料，如公司的電話、地址，當然也不屬於個資法所規範的範疇。



NFT騙局以及安全建議

2021 / 12 / 27 編輯部
最近似乎每個人都在談論NFT(Non-fungible tokens)。你跟上這波潮流了嗎？最近它們的火爆也重新定義了藝術市場，許多人都對它們感到非常興奮，不過騙子也是一 利用NFT來詐騙很多人！
本文將會介紹一些常見的NFT騙局，並分享如何避免它們的方法。

非同質化代幣（NFT）是具備代表所有權數位簽章的藝術品（實體或數位）。它們可以被視為數位資產，也可以像加密貨幣（比特幣、以太坊等）一樣作為貨幣使用。不同的是，每個NFT都是獨一無二的，無法被取代或複製，這就是為什麼它們現在很受藝術愛好者、遊戲玩家和虛擬地產人士的歡迎。

五種常見NFT騙局
•#1 – 假NFT網站
如果你對投資NFT感興趣，首先需要找到可以買賣NFT的地方。在網路上搜尋時，會出現成千上萬的搜尋結果，但其中有許多是假的NFT交易網站。要區分這些詐騙網站和真網站可能很困難，因為通常看起來都非常相似。
首先，詐騙網站上沒有合法的NFT，所以如果你在上面買NFT就只是在浪費錢。更糟的是，詐騙者可以記錄所有你在網站上輸入的資料。通常你只需要提供MetaMask錢包地址就可以進行交易，但詐騙者可能會要求你提供以太坊錢包的助記詞（加密貨幣錢包的主密鑰），並用它來入侵你的錢包並竊取你所有的加密貨幣。

•選擇合法的NFT交易網站
保持安全最簡單的方法是選擇合法的NFT交易網站。有許多不同類型的NFT，體育、電子遊戲、虛擬地產等等。除了最知名的NFT交易平台OpenSea，底下列出一些其他合法的NFT市場/NFT收藏網站：

- **藝術類NFT**
  - Super Rare
  - Foundation
  - Nifty Gateway
  - Rarible
  - Zora
  - Mintable

- **運動類NFT**
  - NBA Top Shot
  - Sorare

- **遊戲類NFT**
  - Axie Infinity
  - Street Fighter
  - Myth.Market
  - Treasureland
- **虛擬地產NFT**
  - Decentraland
- **推特貼文NFT**
  - Valuables

•#2 – 假優惠

詐騙者冒充知名NFT交易平台來傳送假電子郵件給你，聲稱有人為你的NFT出價。他們會要求你點擊內嵌按鈕：

與之前所報導的所有網路釣魚詐騙一樣，這按鈕會導向釣魚網站。假網頁會要求你連結錢包並提交你的助記詞。詐騙者會記錄這些資料並侵入你的錢包，竊取你所擁有的一切！

#3 – 假技術支援

除了假優惠通知外，假客戶服務/技術支援也是常見的詐騙手法。 **透過Discord**

想像一下，當你遇上技術問題並在Discord上尋求幫助時，出現自稱來自OpenSea的人來拯救你。

假技術人員（詐騙者）可能會要求你分享螢幕來檢查發生什麼事，從而讓你在無意間洩露了加密貨幣錢包的憑證。在這個時候，他們可能會截圖你的助記詞（你錢包的回復密鑰）或連結它的二維碼。詐騙者也可能將你導到看似OpenSea官方網站的網頁，要求你輸入詳細的個人資訊。你知道接下來會發生什麼了。不要上當！

•透過電子郵件

在其他案例中，詐騙者會發送關於你OpenSea帳號/NFT收藏的假安全警報。同樣地，他們會要求你點擊內嵌的釣魚連結。不要被騙了！

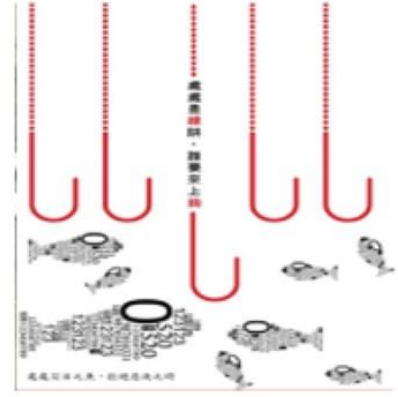
#4 – 假贈品

詐騙者冒充成知名NFT交易平台的員工，透過社群媒體（如Discord或Telegram）聯繫你，聲稱正在舉辦贈品活動。只要你轉發贈品資訊並註冊活動（在詐騙/釣魚NFT網站上），就會得到免費的NFT！當你嘗試連結MetaMask錢包時，你的憑證資訊將會被盜。

#5 – 假NFT專案（抽地毯詐騙）

每天都有許多新NFT專案出現，像是Squid – 以熱門Netflix韓劇魷魚遊戲為名義的新數位代幣。但當它的價格到達頂峰時，它變成了「抽地毯（rug pull）」詐騙 – NFT無法流通。擁有者無法賣出代幣，導致其價格在短時間內暴跌。在這類騙局中，唯一獲利的是數位代幣創造者。

其他案例還有愛情投資詐騙。這些愛情騙子會誘騙受害者投資一些NFT專案。他們可能會發送給你連向假NFT網站的連結，或要求你匯款給他們。要當心！



保護自己不要落入NFT騙局的方法

1.檢查價格。如果一個網站上的NFT報價遠低於OpenSea等合法網站上的報價，則可能是一場騙局。

2.檢查驗證標記。大多數合法NFT賣家的使用者名稱旁邊會出現藍色勾勾標記，並且會清楚列出收藏屬性。

3.檢查聯絡地址。它應該說明NFT是在哪裡鑄造。你可以查看創作者網站來確認資訊的真實性。

4.需要幫助時請聯絡NFT交易網站的官方客服，而不是在社群媒體上出現的人。

5.小心使用你的錢包憑證資訊，切勿分享你的助記詞（回復碼）。

6.使用合法錢包應用程式和瀏覽器擴充程式以避免網路釣魚。有很多惡意應用程式會冒充成官方應用程式。

7.使用強密碼並啟用雙因子身份認證（2FA）來保護你的帳號。可以試試趨勢科技《個資保鑣》，輕鬆主動監測你的個資是否暴露在個資外洩事件中，避免你的email、密碼、銀行帳號、社群帳號在暗網遭洩漏，防範資料外洩，避免財損擴大。

8.切勿點開來路不明的連結或附件。

本文轉載自趨勢科技部落格。