臺東林區管理處政風室
111年9月號

公務機密
資訊安全維護

資安時事案例

網購小心「LINE Pay」付款！YouTuber遭詐6萬

暑假到想出去玩！當心3大網路旅遊詐騙 騙走你一堆錢

個人資料保護法

公務機關蒐集、處理個人資料的要件

生活中的資安

資安也是安全防護網的一環！日常生活中做好資訊安全管理，保障人權也保護弱勢

數位學習

109年資安故事微電影獎 第1名：三不三藥
https://www.youtube.com/watch?v=Qw2k-HQa6vY

網購小心「LINE Pay」付款！ YouTuber遭詐6萬

Tvbs新聞網 何冠毅 蔣睦宇 2022年7月24日

方便的LINE Pay轉帳，居然也被詐騙集團利用！日前一名YouTuber，在網路上買電子產品，過程中，賣家要求用LINE Pay付款，原本想說有實名驗證的LINE Pay還算安全，就轉了6萬元，後來才驚覺被騙。警方也發現，透過LINE Pay付款的詐騙案件，確實有增加趨勢。

YouTuber劉思欣：「十幾頁的案底吧，點開都是因為網路詐騙，而且幾乎都是臉書加上LINE Pay支付，所以他們應該是詐欺慣犯。」

自拍影片分享自己被詐騙的過程，YouTuber劉思欣用自身經歷，提醒大家要小心這種新型態詐騙手法，而付款方式竟然是越來越方便的LINE Pay轉帳。

YouTuber劉思欣：「他就問說能不能接受用LINE Pay，當時是覺得說這只是一種轉帳方式，而且LINE Pay也是有實名認證應該還好。」

當初在臉書社團要買電子產品，雙方談妥原本打算面交，但賣家說人在高雄不方便，詢問是否用LINE Pay付款，原本想說有實名驗證還算安全，就轉了6萬元給對方，但她直覺不對馬上打給165確認，才發現真的是詐騙。

YouTuber劉思欣：「他們(165)就說這一定是詐騙，因為他們有很多案例都有打電話來，但LINE是國外的公司，所以不一定會協助台灣警方去查案件。」

根據刑事局統計數據，去年詐騙案總數是24724件財損高達56億，而會用上LINE Pay的多半是網購詐騙，也有5623件金額3億7千萬元，警方發現LINE Pay詐騙有在增加，加上是國外公司警方調查困難，越來越多被用在詐騙付款。

記者何冠毅：「其實LINE Pay本身就有一定程度實名制，在申請時會需要準備手機驗證，身分證以及銀行帳戶驗證，這些都是LINE Pay本來就有的防詐機制。」

除了實名制LINE Pay本身也有設定，轉帳上限單筆少於5萬每天10萬以下，每個月也不能超過20萬，不過幾百幾千的小額詐騙，其實在LINE Pay上才是大宗，但礙於偵辦困難被害人被騙走的這6萬元，目前依然是一去不回。

YouTuber劉思欣：「他說請我一定要去報警，因為這樣的案例夠多，才有可能會LINE公司施壓。」

暑假到想出去玩！當心3大網路旅遊詐騙 騙走你一堆錢

SETN三立新聞網 111.7.27 記者谷庭／台北報導

全球迎來後疫情時代，政府宣布縮短入境隔離天數。為了迎接期盼已久的出遊假期，國內飯店、民宿訂房率大增，更有不少民眾選擇踏出國門，根據桃園機場統計，7月暑假第一天的出境人數便爆衝3倍，但也出現了旅遊相關的網路陷阱，資安廠商趨勢科技彙整三大旅遊網路資安危機，以及各種個資外洩遭盜用的風險。

趨勢科技表示，近來有知名旅遊網站、旅宿業者遭到駭客入侵，導致民眾個資外洩。提醒民眾如果接獲自稱是旅遊業者或訂房網站的電話，請先向業者求證，千萬不要輕易透露個資或卡號，並應定期檢查信用卡刷卡紀錄、定期更改密碼，同時建議民眾可使用免費個資保鑣App檢測自己的Email、電話、信用卡號碼等個資是否在暗網遭外洩過，成為詐騙集團的目標。

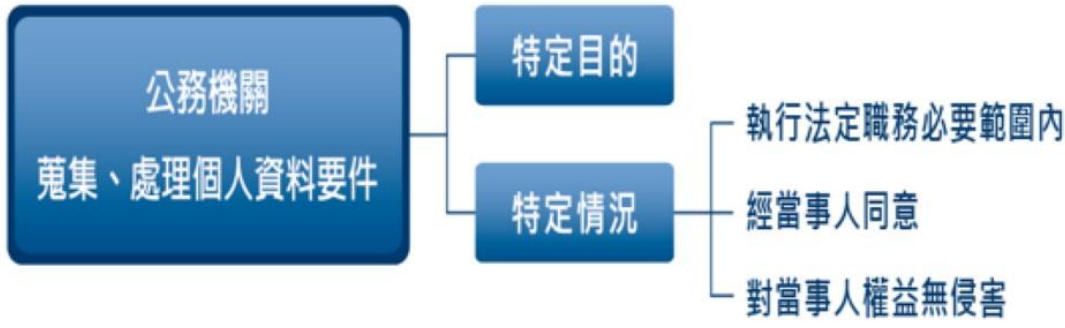
根據趨勢科技最新調查數據顯示，自今年3月政府頒發防疫補助紓困方案以來，已有近千筆防疫補助相關詐騙事件發生，有民眾就收到假冒政府發布防疫補貼的簡訊通知，簡訊內附帶假的網址吸引民眾點擊，目的就是要騙取個資、信用卡資訊和網銀帳號密碼等銀行帳戶登入資訊，甚至篡改驗證資料進而轉出大筆資金。

趨勢科技表示，民眾應一律使用政府官方機構提供的連結網址，直接在官網申請相關補助，切勿點取不明簡訊與連結，同時安裝行動安全防護加強行動裝置安全，以免還未領取到補助，錢財就先被詐騙集團盜領。

公共場所的資安問題層出不窮，無論是在國內外，飯店、機場或是火車站等場所皆有提供免費Wi-Fi，在享用網路的便利之餘，別忘了公共Wi-Fi隨時都可能伴隨著風險，特別是透過未經加密的公共Wi-Fi傳送資料，將使駭客有機會隨時連上開放網路，掌握使用者上網行為，盜取信用卡、帳密等個資。

趨勢科技建議民眾出門在外如必要使用公共Wi-Fi，可以先關閉自動檔案分享/同步功能、使用VPN應用程式來保護Wi-Fi連線，或安裝防毒軟體工具來封鎖惡意網址，簡單的小動作可防止隱私被偷窺、個資遭外洩。

公務機關蒐集、處理個人資料的要件



【沒有侵害當事人的權益】

舉例而言，如果某公立學校基於教育行政目的蒐集了學生的個人資料，卻也順便蒐集學生的指紋，這個指紋是與教育行政無關的資料，此時，該公立學校蒐集學生的個人資料已侵害學生的資訊隱私權，這樣的蒐集是不被允許的。

資安也是安全防護網的一環！
日常生活中做好資訊安全管理，保障人權也保護弱勢

圖／rawpixel @ unsplash

公益交流站 文／Yi-Chia Chen

在臺灣，資訊安全是一塊很容易被忽略的領域。聽到資訊安全、隱私權等話題時，很多人第一個反應往往都是：「我沒有做壞事，幹麻怕別人看。」對此，記者 Glenn Greenwald 在一次 TED 演講裡分享，每當他聽到有人這麼說，都會馬上拿出一支筆，寫下自己的電子郵件，並要對方回家之後將自己所有的電子郵件，包括工作及私人電子郵件的帳號密碼都寄給他，好讓他在線上觀察他的一舉一動。當然，從來沒有人應他的要求這麼做。

資訊安全是基本人權

資訊安全可以細分成很多種類，個資保護便是其中一環。去年 5 月，針對個資保護，歐盟開始實施《個人資料保護規範》（General Data Protection Regulation， 簡稱 GDPR），只要是來自歐盟國家的人，都會受到這項法律保護。如果組織成員裡剛好也有歐盟國家成員，或是會經手處理到歐盟國家成員的相關資料，都得依這項法律做出適當調整。

根據 GDPR 第 4-1 條規定，個人資料包括任何得以辨識自然人的資料，如姓名、身分證字號、生理及心理狀態，就連經濟、文化等社會特徵都包含在其中。任何一項資料遭到洩漏或被有心人士不當利用，都有可能使一個人的榮譽與名譽受到攻擊，進而違反聯合國《世界人權宣言》第 12 條裡訂定關於人的基本權利：「任何人的私生活、家庭、住宅和通信不得任意干涉，他的榮譽與名譽不得加以攻擊。人人有權享受法律保護，以免受這種干涉及攻擊。」

而既然個資保護牽涉個人隱私，出問題甚至會影響他人的基本權利，身為非營利組織的工作者們更應該正視這項議題，抱持「以人權為本的工作方法」（Human Rights-based Approach）之工作精神，做到知行合一。

維護資安，不止保障人權，也保護弱勢

為了避免監控，人權團體所關注的人權捍衛者需要特別小心，此外，一般社工所接觸的案主也都是社會上特別需要保護的一群人，單位甚至時常需要收集他們的個人資料做後續評估，若資安管理出了狀況，不僅案主的名聲會受到負面影響，嚴重的話，如人權捍衛者們，可能還會被企業、政府等擁有較大勢力的團體以更惡劣的手段加乘傷害。

或許有人會提出質疑，認為其經手的個案都不是名人，不會有人想利用這些資料。關於這點，也許可以想想看：對有犯罪意圖的人來說，一旦決定要偽造他人身分犯案，其會選擇名人，還是默默無名的人？哪一個比較容易成功？而這些默默無名的人，本身就屬於社會上相對弱勢的一群人，若身分遭偽造，淪為他人的犯罪工具，用來不當借貸、盜刷，甚至其他更嚴重的違法行為，後果恐怕難以想像。

2016 年時，勞動部就曾爆出其就業網站「臺灣就業通」遭駭，疑似有 3 萬多筆個人資料流出，而這些登錄資料便是來自社會上相對弱勢的族群。當時就有人質疑政府的公共服務系統不夠穩固；此外，也有人呼籲社福界應該就這警鐘好好調整工作模式，並投入資安保護資源等，加強資訊安全。然，事發至今已經 3 年，社福界對於資安管理的知識又增長了多少呢？

資安管理從日常生活著手，養成資料維護的好習慣

1. 電子郵件：上網檢查信箱安全、定期更換密碼

電子郵件是一般工作上最常用到的工具，而許多個資外洩也都是從電子郵件開始。

首先，可以透過 Have I Been Pwned（HIBP）這個網站做第一步檢查。 HIBP 是由微軟區域經理 Troy Hunt 所開發的網站，裡頭收錄這幾年來曾經被駭客竊取、並公布在網路上的名單資料。只要輸入電子郵件地址，馬上可以知道自己的資料有沒有外洩。

若檢測結果為綠色，代表目前在網路流傳的資料外洩名單裡面，沒有你的電子郵件資料；若檢測結果為紅色，則表示情況不妙，該網站甚至會顯示你的資料是在哪一波被駭的服務中遭到洩漏，此時，記得趕快更改信箱密碼。

若想再更保險，則可以考慮更換安全性更高的電子郵件系統，如 ProtonMail、Thunderbird 等。但倒也不是換了一次密碼和整個系統後，就可以從此相安無事，使用者還是必須養成定期更換密碼的習慣，也別忘了在寄出郵件前謹慎加密，因為只要郵件加密，就算未來系統被入侵，入侵者也只能截取到一長串的隨機字元，可以確保重要通訊資料不至於外洩。

2. 即時通訊軟體：選擇使用安全性相對高的通訊軟體

現在人手一支手機，網路也隨處可得，即時通訊軟體成了大家所仰賴的生活必需品。不只是私生活領域，很多人也會透過即時通訊軟體聯絡公事，自然也應該是非營利組織工作者的「防疫」重點。

2016 年時，國際特赦組織就曾經針對 11 間科技公司旗下的即時通訊軟體，依據加密程度排名。而這 11 間科技公司及其通訊軟體分數由高到低依序為：Facebook（Messenger、WhatsApp）、Apple（iMessage、Facetime）、Telegram（Telegram Messenger）、Google（Allo、Duo、Hangouts）、Line、Viber Media（Viber）、Kakao（KakaoTalk）、微軟（Skype）、Snapchat、Blackberry（Blackberry Messenger）、騰訊（WeChat、QQ）。其中，工作上較多人用的 Skype、Google Hangouts、WeChat 則完全沒有加入端對端的加密技術， Facebook Messenger 則沒有預設端對端的加密技術。

網站 Secure Messaging Apps Comparison 也針對 Allo、iMessage、Messenger、Riot、Signal、Skype、Telegram、Threema、Viber、WhatsApp、Wicker、Wire 等共 12 個即時通訊軟體做出評比，而裡頭的 Signal、Threema 及 Wire 是網站開發展比較推薦使用的軟體。但他也提醒，如果想完全避免政府監控，則應該使用 Threema 及 Wire 。

3. 瀏覽器：選擇維護用戶隱私的網頁瀏覽器，或加裝外掛軟體

瀏覽器是上網必經的媒介，可以透過不同的網頁，搜集用戶的各項資訊。如 Google 就利用 Chrome 搜集了大量的瀏覽數據，轉賣給廣告商，讓廣告商可以精準的對用戶投放廣告。雖然在 Google 的維護下， Chrome 有著一定的安全性，但在隱私方面就不太能有所指望。

擔心資料被大公司任意搜集，可以參考為大眾提供隱私保護的社群計畫 privacytool.io 所推薦的 3 個瀏覽器：洋蔥瀏覽器（Tor）、火狐（Mozilla Firefox）以及 Brave。其中，Tor 洋蔥瀏覽器提供額外的匿名層保護，速度慢但隱匿性很高；Mozilla Firefox 則以快速且尊重用戶隱私聞名；而 Brave 則強調自動封鎖廣告與追蹤器。

若不想更換瀏覽器，也可以選擇瀏覽器外掛軟體，像是 Privacy Badger、 uBlock Origin 與 Disconnect，保護上網隱私。
Wire 。

4. 雲端硬碟：使用遵守國際個資規範的雲端服務，提升資料安全

除了各式實體硬碟，很多人也會將資料儲存雲端硬碟上。雖然只要將檔案傳上網，儲存在第三方的伺服器中，就已沒有隱私可言，然而選擇重視資料安全的雲端服務，仍有助於提升使用上的安全。

Tresorit Send 便是一款強調其為「已知的宇宙間」最安全的檔案傳輸工具及儲存空間，不僅提供點對點的加密，也遵守瑞士法律及歐盟 GDPR 的相關規範。它支援最大 5 GB 大小的檔案，不過若使用免費版本，檔案只能保存 7 天，或在下載 10 次後便會自動失效。

5. 虛擬私人網路（VPN）：雖針對網路提供額外保護，仍不保證安全

VPN 的全名是 virtual private network，意思是虛擬私人網路，可以對隱私提供額外保護。雖然大多數的 VPN 都採不記錄用戶活動的策略，但可不是有了 VPN 就一定安全。中國就曾有用戶反映，在特定的政治集會期間，其 VPN 遭受干擾、無法連接。目前市面上免費、且比較安全的 VPN 有 hide.me 以及 ProtonVPN，前者的供應商在馬來西亞，後者則在瑞士。

6. 其他個資安全相關配套措施

如果還是不確定該從何做起，也可以參考 Security Planner。 Security Planner 是由加拿大多倫多大學團隊 Citizen Lab 所開發的計畫，提供大眾簡易的資安建議。

以提問的方式，從一般會使用的軟硬體設備，到個人較注重的資安問題，逐步幫大家分析並找出合適的資安方案。
資安維護需要全民的重視，並共同維護

如同交通安全、住家安全、校園安全等，資訊安全和上述任何一種安全一樣，需要大家重視，也需要大家共同維護。尤其當它涉及個人隱私、關乎人權時，更應該小心看待。如果我們離開辦公室、住家，都會習慣上鎖，線上資料也同樣不容輕忽，試想：不管是在辦公室還是住家，只要有人沒有注意，忘記上鎖，安全防護網便會出現漏洞。那麼，資訊安全做得不夠完全時，有任何人怠忽職守，那是不是也會招來同樣的問題呢？