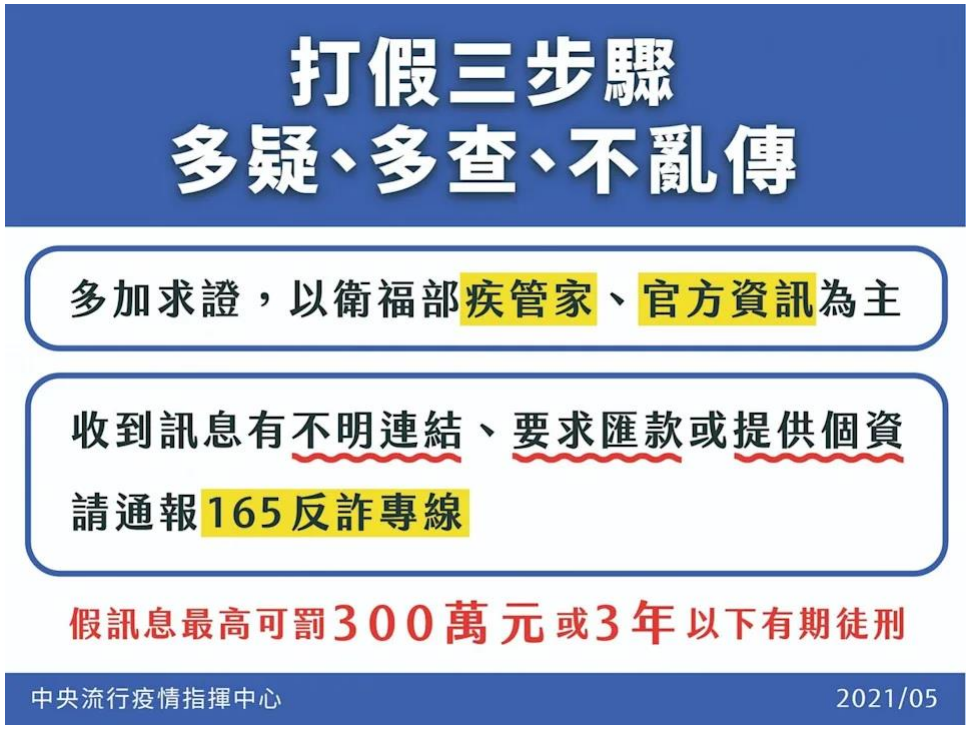
臺東林區管理處政風室
110年10月號

公務機密
資訊安全維護

反詐騙電話165



資安時事案例

衛福部30秒問卷調查領取800福利金？
冒名網站，切勿提供個資

臉書網購詐騙 實品差超大笑翻網友

個人資料保護法

為何需要制定新版個人資料保護法？

生活中的資安

因疫情帶來的資安破口，我們該做些什麼？

數位學習

107年資安動畫金像獎
一蘋如洗

【詐騙】衛福部30秒問卷調查領取800福利金？當心冒名網站，切勿提供個資

MyGoPen 110.9.22

網傳「30秒問卷調查 領取800福利金」的貼文與聲稱是衛福部的「民生問卷專區」網址。經查證，近期衛福部並無推行此問卷，警方指出，一般政府機關的訪問調查並不會用連結網址的方式，因為會有詐騙集團做假網址的問題，衛福部更提醒民眾勿上當受騙。

在社群平台流傳：

查證解釋：

對此 MyGoPen 致電 165 反詐騙專線詢問衛福部是否有相關問卷調查，警方表示目前並沒有收到衛福部有相關公文，一般來說政府單位會有明確的行文，經警方查詢，衛福部近期並沒有和網傳相關的「民生問卷」，不過有關於國民健康訪問的調查，時間從今年 4 月到 9 月，主要是了解國人健康狀況，調查方式是隨機抽選樣本，然後派訪問員進行訪談。

經民眾回報的內容，發現主要手法是透過問卷文案，引導民眾加入不明的 LINE 帳號，並試圖取得銀行帳戶等個資。至於網站也並非衛福部的網域，偽裝衛福部的 mohw 網址以及冒用衛福部的標誌 LOGO，也請民眾切勿點選或填任何資料。

這個 LINE 帳號也沒有任何官方認證標誌，主要會藉此說要民眾拍傳「銀行存摺照片」好來安排匯款，這都要特別小心！請不要將個人存摺提供出去。

警方指出，通常政府機關的訪問不太會用連結網址的方式，一般是先在各縣市地區隨機抽樣完後再由訪問員致電、發文聯繫做電訪或面訪，基本上不會用網址，因為會有不確定網址是否正確的情況，有些詐騙集團會做假網址，比如說數字 1 用英文字母小寫的 l 、英文字母 m 和 n 、數字 0 和英文字母 O 諸如此類的。

但為了謹慎起見，警方建議還是要再聯絡衛福部確認是否有相關的訪問調查，因為有時候政府單位公文過多，難免有疏漏，所以 MyGoPen 也致電衛福部，衛福部確認並無此事，提醒民眾勿上當受騙。

今年 5 月衛福部亦有發布相關新聞，指出有民眾反映疑有詐騙集團假冒疫調人員向民眾騙取個資，中央流行疫情指揮中心提醒大家應提高警覺，若有疑慮可利用刑事警察局 165 反詐騙諮詢專線查證。

資料來源：
衛福部 - 遇到詐騙集團假藉疫調騙個資，指揮中心：可向165反詐騙專線求證
單位諮詢： 內政部警政署 165 反詐騙諮詢專線
衛生福利部

臉書網購詐騙 實品差超大笑翻網友

▲趨勢科技觀察，大量假冒知名月餅商家的不肖業者，使用與店家相似的帳號名稱，吸引不知情的消費者下單購買。（圖／趨勢科技提供）

記者賴志昶／台北報導 110.9.21

看準民秋連假網購需求增加，詐騙集團也伺機搶發中秋財。根據全球網路資安品牌統計，在台灣網路詐騙類型中，「一頁式購物詐騙」占比達58%，為所有類別中最高，光在5至8月就偵測到逾377萬筆。

針對一頁式購物詐騙主要特徵，根據全球網路資安品牌趨勢科技觀察，該類型詐騙是擅用知名店家相似名稱，並使用官方網站商品圖片、影片，同時強調24小時到貨或免排隊，並主打價格低於市場行情，還提供限定期間免運費等好康資訊，至於網頁方面，則資訊簡陋，沒有公司地址、客服電話等，且夾雜簡體字或使用非本地用語。

趨勢科技提醒，民眾瀏覽各式購物網站或廣告時，應提高警覺心多留意查證，盡可能避免在非官方網站購買商品；為提供民眾更全面性的反詐騙服務，該品牌現更推出「防詐騙瀏覽器」擴充功能，能夠同時支援Chrome、Safari和Edge瀏覽器，為使用者自動評測瀏覽網站安全性，自動警示阻擋各種詐騙網站和釣魚連結，攔截廣告與第三方追蹤，協助檢查歷史紀錄並清除可能風險，讓民眾安心上網無虞。

為何需要制定新版個人資料保護法？

資料來源: iThome

因舊法「電腦處理個人資料保護法」的保護範圍有限，無法符合現今社會型態，跟不上國際對於個人資料保護的潮流。不論就保障人民權利，或是在國際上與其他國家的合作往來，舊法都顯得不合時宜。

擁抱陽光 輪轉幸福

因疫情帶來的資安破口，我們該做些什麼？

2021/09 /15 投稿文/ 科技大觀園

COVID-19 疫情籠罩全球，台灣也在今年初首度迎來疫情高峰，在疫情影響下，人們的生活型態出現大幅改變，遠端網路服務需求攀升同時也促使相關資安威脅升溫，究竟疫情帶來的資安問題有哪些？人們又該如何預防呢？

遠距工作帶來的資安風險

談到資訊安全，許多人第一時間想到的可能是大企業面臨的問題，但其實個人生活中也可能隨時遭遇相關威脅不自知，連帶造成後續許多問題，而讓個人生活與工作更加密切的遠端作業則更加深化其中存在的風險。

臺灣大學資訊工程學副教授蕭旭君指出，原有工作型態下為了防止機密外洩，多數企業都會在網路邊界系統設有防火牆、偵測系統等多套措施，內部網路與系統也會部署偵測機制加以重兵防護，即使有惡意程式入侵也能夠迅速發現，或甚至內部網路根本不對外開放，但隨著遠距工作型態出現，迫使企業網路必須接受來自公開網路的連線，也導致原本的防線出現破口。

由於必須開放內網給在外員工連接，許多企業會要求員工使用 VPN 連接到內網，儘管 VPN 確實能提供相對安全的連線環境，但這也讓 VPN 變成很明顯的目標，許多報告都顯示面向 VPN 的攻擊大幅增加，2020 前十大常被利用的資安漏洞幾乎都與和 VPN 有關。

遠端作業型態下，員工必須使用許多軟體協助工作，而個人電腦也多有其他用途，由外部連到企業內網的網路節點增加，這一切都使得遠距工作需要防護的面向變的更加廣泛。當企業原有的防護難以延伸到員工自己的網路和設備上，一旦員工在基礎資安防護上出現疏漏，如使用常用密碼登入 VPN，或個人電腦曾經下載過一些惡意軟體，便可能導致潛在的資安隱憂出現。

值得一提的是儘管更不常被視為目標，但國外許多研究都發現，與具有充足資源的大企業相比，疫情可能帶給中小企業更大的資安挑戰，蕭旭君解釋，中小企業可能被看做是容易得手的目標，或成為勒索軟體無差別攻擊下的受害者，或被當成攻擊其他客戶的破口或跳板，對於資源較有限的公司來說要避免受害，最好的方式就是確定自己至少有達到基本資安防護。

除了與大公司有業務往來的上游廠商被當成跳板的『供應鏈攻擊』較難以應對，多數中小企業面臨的攻擊都是來自簡單的地方，像是不要亂點釣魚信件、注意連線加密（HTTPS）、確保密碼不重複且注意洩露、軟體定期更新等，在攻擊者利益導向的目的下，只要不要讓攻擊能夠太簡單侵入，就可以做到有效防護。

「雖然這些都已經講了很多年，但因為容易疏忽還是可能被當成破口。建議企業在有限資源下從簡單地方入手比較容易達成，如果有額外資源還可以做額外防範。」

防疫生活重心轉變

在遠端工作上面臨的資安風險之外，防疫帶來的生活重心轉變也成為攻擊者關注焦點。以網路購物為例，過去數年網購詐騙就已經是 165 全民防騙網上的常客，在防疫提倡維持社交距離情況下，牽動的網購風潮更加推升了這種情況。

蕭旭君解釋，網路購物的資安風險主要與個資洩露相關，當攻擊者拿到個資後為了轉換獲利，便可能透過詐騙電話與受害者聯繫，利用獲取的個資取信於人，近一步詐取相關財務，而台灣購物網站過去便經常傳出個資外洩的事例，更別提近期社群媒體上盛行的網路拍賣，在金流沒有受到控管下更加沒有保障。除此之外，疫情也促使許多實體店家展開線上販售服務，在上線時間匆促下，如果程式碼沒有妥當檢查，一旦被攻擊者加以利用，同樣也具有個資洩露風險。

至於經常被拿來討論的 QR Code 簡訊實聯制，雖然大幅提高便利性，但社會上仍有少數質疑可能遭濫用的聲浪存在。蕭旭君認為，從民眾角度來說，難免擔心足跡是否會被收集做為他用，但事實是各式做法都存在不同隱私隱憂，民間版本同樣也存在個資被作為廣宣用途的疑慮，然而實際情況是，所有開發者必須在安全性、民眾接受度跟資安上做出權衡，民眾可以基於公開資訊，自行選擇更傾向的追蹤方式來做好防疫並保障隱私。

因應防疫新興的遠端網路服務，攻擊者利用人們迫切想要吸收疫情相關資訊的心態，散佈假消息到處傳播，甚至假裝疫調騙取個資的情況都時有耳聞。蕭旭君提及，未來可能出國必備的疫苗護照、檢測證明也是國外熱門議題，除了牽涉個人隱私，是否會被偽造、如何防範被偽造也是國際焦點，顯見防疫下的資安議題仍不容小覷。

不存在沒有資安風險的網路服務

說了這麼多，許多人可能會好奇從資安的角度來說，有可能會存在完全沒有資安問題的網路服務嗎？針對這點，蕭旭君表示，以實務角度來說是沒有辦法做到這點，「除非你不上網，那當然就沒有網路資安的問題」。

蕭旭君解釋，在資安攻防中，需要對威脅做出具體假設並針對特定攻擊者進行重點防護，然而實際生活中有太多事情沒有辦法掌控，像是無法控制使用者如何使用系統，一旦行為與預期不同便可能出現意外漏洞。同時資安防護成本有限、對電腦的效能有較高需求前提下無法加上太強大防護，這些都會導致實務上無法防範所有攻擊。在具有太多假設不確定性下，無資安隱憂的網路服務基本上是不可能做到。

「資安攻防中有特定對手，在資訊安全進化的同時，攻擊者也會進化、會成長，就算能防範已知威脅，未來還是會有新攻擊出現。」

當然，這並不意味著我們對資安攻擊便只能認份接受，就像生活中的大小意外一樣，只要做好足夠防範並保持靈活想法就能隨時應對處理問題。拿學校遠端教學來說，線上測驗同樣可能為教授們帶來代考問題。在保障考試公平性和學生隱私的權衡中，有些單位使用監考軟體，一些則取消考試改用其他方式評分，或像蕭旭君一樣選擇採取線上考試但讓同學可以翻書找答案。

如上所述，資安防護其實有許多手段可供選擇，蕭旭君強調，實務上資安防護就是風險管控，如何盤點自身弱點並利用手上有限資源進行最佳部署減少風險才是最重要的。只要做好基礎防護提升攻擊難度，在希望獲利的前提下當攻擊成本提高，攻擊者便可能打退堂鼓或轉換目標。

攻擊並不可怕，更令人擔憂的是被攻擊了還處在未知情況，「至少做到被打要覺得痛，才能更好做出接下來的反應。」

將資安防護當成防疫看待

即使未來疫情告一段落，可想見帶起的遠端風潮仍會持續，資安環境提升對未來的影響與重要性無言可喻。對於台灣資安環境，蕭旭君整體還是樂觀看待， 她表示隨著資安被拉升到國安層級，國際上對資安重視度越來越高，台灣產官學也越來越重視，整體投入的資源及人力都有顯著提升。

做為大學副教授，蕭旭君明顯感覺到近年來對資安有興趣的學生越來越多，在政府稽核標準要求提高下，企業方對資安人才的需求也持續升溫，近期教育部舉辦的資安暑期課程參與學生數明顯增加，參與媒合的廠商意願也提高，隨著台灣團隊參加國際資安競賽等正面報導傳出，人們對資安有更多正面應用的印象也提高相關興趣。

台灣由於地理位置特殊，潛在攻擊者特別強，出發點也並非僅出於利益導向，在政治意圖引領下防禦起來更為困難，近年針對關鍵基礎設施的攻擊、大企業的勒索也陸續傳出，蕭旭君認為，未來大家更需要謹慎因應並更重視資安，「資安不只是政府部門或企業的事情，對一般人來說也很重要。」

由於日常較少涉略，許多人對於談及『在個人生活中應對資安』可能會明顯卻步或感覺抗拒，但其實這並不是這麼困難的事情。在個人生活中就像前面提醒大家的一樣，確保網站密碼強度足夠且不重複，盡量減少留下個資機會、連線時注意保護加密、不要打開奇怪信件並關閉自動預覽，這些基礎原則就已經提供足夠的上網保障。

蕭旭君表示，在疫情影響下，現在大家對疫情防護策略較為熟悉，隔離、篩檢、疫調、打疫苗…等，而在她看來，這些防疫概念其實都可以對應到資安防護上，只要簡單想像並比照辦理，做好『防疫』並『增強體魄』，就能做到基本資安防護。

「如何保護自己不受 COVID-19 的侵襲，你就用同樣的策略去確保面對個人資安保護。」

本文轉載自科技大觀園