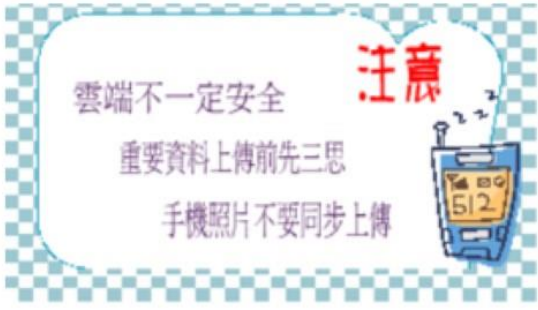
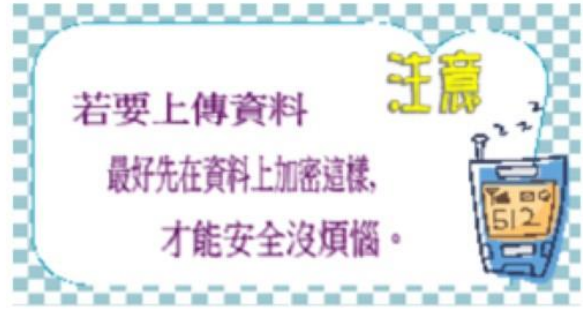
公務機密
資訊安全維護





資安時事案例

公共WiFi藏資安風險

盤點 7 種常見的資安風險，看看你犯了哪些錯？

個人資料保護法

公務機關個資安全維護

生活中的資安

我們與資安風險的距離！數十兆元地下經濟來自你我的輕忽

數位學習

103年度資安動畫金像獎 ：
上傳決定害死你

公共WiFi藏資安風險

- 公共WiFi釣魚，黑色產業鏈非法賣訊息
  - 現代人離不開手機，隨時都想上網，但公共WiFi暗藏資安風險，特別是些沒設密碼的公共WiFi。如果連上駭客設置的偽冒的公共WiFi基地台，使用者登入網站的帳號、密碼都會被駭客攔截及賣掉
  - 萬一駭客進入您的手機，可能導致私人郵件、商業郵件或行動支付帳密洩漏，賣給非法人士。大陸駭客的黑色產業鏈，規模高達上百億人民幣
  - 以色列手機保全公司公布全球最不安全的公共WiFI地點，前五名是紐約時報廣場、巴黎聖母院、巴黎迪士尼、舊金山金門公園以及香港海洋公園

專家提醒不需要密碼的公共WiFI可能有釣魚陷阱，盡量避免使用。若真的需要連接公共WiFI，盡量不要操作行動支付或登錄網路銀行，手機、平板、電腦需安裝防毒軟體，另外家用的路由器設定高強度的帳號、密碼以降低風險

資料來源：https://news.tvbs.com.tw/life/615399

盤點 7 種常見的資安風險，看看你犯了哪些錯？

作者 侯 冠州 | 發布日期 2020 年 11 月 19 日

遠距工作、教學成為疫後新常態，對資安威脅也隨之增加。然而，許多人始終認為這些都是企業才應該重視的問題；或覺得就算中毒，直接將電腦格式化、重新安裝作業系統即可。但是，隨著人們對於資訊內容使用方式的改變，在當前手機成為主流使用裝置，互動模式以線上社群服務為主的情況下，駭客發動的惡意攻擊模式也隨之改變。

趨勢科技表示，民眾別以為駭客對於一般人個資不感興趣，事實上，有大量個資內容在網路黑市以高額價格販售給包含色情集團等不肖業者。資安攻擊，其實時時刻刻存在，以下盤點 7 種日常生活中常見的資安風險。

風險一：網路釣魚

網路釣魚可說是最常見的攻擊手法。網路釣魚時常搶搭熱門時事話題，如疫情、三倍券、雙 11 購物等，透過各種管道偽裝，如釣魚簡訊、釣魚郵件、一頁式網頁等，企圖欺騙消費者個資。趨勢科技資深技術顧問簡勝財表示，這種手法常以釣魚郵件將使用者引導至偽裝成真實購物網站、銀行、信用卡公司或網路服務等之合法登入頁面的假網站，藉以竊取使用者在該網站所輸入個資。

簡勝財進一步指出，除了引導至釣魚網站外，其他還有各種形式的巧妙手法，例如誘導使用者安裝惡意應用程式或要求回覆釣魚郵件。先前常見的大量名人粉專遭駭即是透過網路釣魚的方式，駭客透過大量設立偽冒的官方粉絲專頁，在其頁面上 Tag 許多不同名人網紅的 Facebook 粉絲專頁，引導用戶至假冒的 Facebook 登入頁面，要求登入以驗證帳號。

風險二：連接公共 Wi-Fi 要考慮

由於 Wi-Fi 是以電波進行通訊，若是民眾連接到安全措施不完備的 Wi-Fi 或是駭客故意設置的假 Wi-Fi，例如駭客創造與公共 Wi-Fi 名稱相似的假熱點，讓使用者在不知情的狀況下登入 Wi-Fi，以竊取個資。換言之，民眾在使用公共 Wi-Fi 的過程中，可能面臨遭受第三方惡意偷窺、通訊內容被監視的風險。

風險三：惡意 App

一般民眾普遍認為手機不會中毒，但是目前非法應用程式已是智慧型手機的主要威脅之一，在應用程式商店上也可能有非法應用程式，駭客會利用惡意網址或惡意 App 盜取手機上的重要資料，民眾用手機遭到詐騙的機率很高。

風險四：軟體漏洞攻擊

因軟體漏洞而遭受攻擊，惡意軟體或惡意應用程式會針對作業系統等安全漏洞進行攻擊，例如駭客利用瀏覽器漏洞植入病毒，或是駭客透過網路直接攻擊系統漏洞（類似像 WannaCry 勒索病毒）。

風險五：瀏覽被入侵的網站或惡意連結，被導向下載惡意程式
民眾一旦瀏覽遭受惡意入侵的網站或是點擊惡意連結，可能會導致裝置被下載惡意程式，而遭受勒索或重要資訊外洩。

風險六：詐騙訊息

詐騙訊息也是十分常見的手法，駭客透過電話、網站導向、彈出式視窗廣告、釣魚郵件等發送詐騙訊息，接觸潛在目標。像是在社群媒體上散播假免費服務電話、假技術支援網站連結等，用來誘騙在線上搜尋技術支援資訊的使用者點入網路釣魚網站或撥打免費服務電話，取得受害者個人身分資料或讓受害者為其「服務」付費。
簡勝財說明，此外，性勒索也是常見詐騙訊息，例如駭客透過交友軟體或社群加入受害者好友，發送免費觀看成人網站為誘餌的詐騙訊息，在受害者點擊後，警告受害者觀看色情影片過程已經被側錄並要求贈金，而手機可能也會因為瀏覽受感染的色情網站面臨被植入勒索軟體的風險。

風險七：不安全的家庭路由器或 IoT 設備

隨著家庭聯網設備越來越多，除了為生活帶來更大的便利性，卻也為駭客提供更多的入侵節點。智慧家庭生活日趨便利，家用網路潛在資安風險也持續升溫，一旦家中路由器安全性遭破解，駭客可以隨意入侵各式連網裝置，使家中成員的資訊安全暴露在高風險下，導致智慧連網裝置遭竊聽、誘導至非法網站而遭詐騙或感染病毒，使得民眾隱私外洩，進一步造成財產損失。

公務機關個資安全維護

- 個資法§18：公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。
- 施行細則§12：規定了十一項具體的安全維護措施內容。
- 施行細則§25：規定「專人」必須具有維護能力，並應接受相關專業之教育訓練。

案 例

我們與資安風險的距離！數十兆元地下經濟來自你我的輕忽

作者 Pin | 發布日期 2020 年 11 月 19 日

前陣子一則網路新聞掀起了網路的話題——一個由中國品牌「囚愛」開發的男性貞操帶，被發現控制貞操鎖的 App 有安全漏洞，若遭駭客鎖定，駭客可以遠端操控貞操帶，導致貞操帶沒辦法解鎖。如果用戶不幸碰上被鎖，就只能透過人工切割的方式解鎖。

這則新聞多被大家視為獵奇的事件，看看笑過就算了。然而，這則新聞背後卻有其重大意義，也就是每個人資訊安全的曝險都越來越大了。試想，把「貞操帶」替換成個人電腦、個人手機、家中的路由器、家中的寵物攝影機、家中寶寶攝影機、家裡的智慧電視、家庭監視器、聯網冰箱、聯網冷氣、聯網洗衣機，甚至是可以用 App 操控的門鎖等等，這些裝置雖然都需要帳密，但資安專家表示，許多使用者甚至沒更換過原廠密碼，駭客要入侵簡直輕而易舉。

一般民眾可能並未警覺，光是從一張在 Instagram 的照片，駭客就可以找出個人所在位置與相關個人資訊，更何況是上述這些產品，一旦遭鎖定，個人資訊就直接攤在駭客眼下，損失的可能將不只是造成「皮肉痛」的切割解鎖，而是個人資訊的曝光、財務的損失，更甚者是人身安全的危害。

而你我身旁的資安風險只會越來越高。「因為疫情的影響，全球網路使用的頻率增加了、在家上班越來越普及，這個情況導致網路攻擊的頻率也跟著升高。」TeamT5 執行長蔡松廷表示。駭客攻擊在 COVID-19 疫情發生後上升的態勢，早已是資安業界的共識。

網路犯罪一年「產值」比蘋果公司營收高出 5 倍

這些包含勒索軟體、資訊竊取在內的網路犯罪商機究竟有多大？根據一份網路犯罪經濟的學術研究顯示，網路犯罪經濟一年高達 1.5 兆美元（約新台幣 43 兆元）。這個數字比全球最會賺錢公司之一的蘋果，在 2019 年的 2,600 億美元營收還多了 5 倍以上。

「在家工作」掀起 VPN 需求，企業內網資安面臨嚴重考驗

不只是個人資訊安全風險越來越高，企業面臨的資訊安全風險也同樣逐年高升。尤其在疫情發生後，企業內網的安全性受到了「在家工作」趨勢的嚴峻挑戰。

蔡松廷就指出，疫情後可以看到企業資訊安全可攻擊的面向增加，特別是因為員工必須在家上班，家中電腦的資安防護並未像企業內部電腦這麼高，加上頻繁使用 VPN，連線到企業內網的裝置大幅增加，使用的複雜度增加，對於公司內部負責網路裝置的人員來說，要判讀員工使用 VPN 是否造成異常的難度也大幅提升。

事實上，今年在疫情發生之後，就有許多企業與政府機關，因為 VPN 的使用，被駭客攻入內網造成資安的威脅。「從 VPN 找破口攻擊，就可以直搗核心，直接朝企業內網下手。」蔡松廷說。

「在家工作」掀起 VPN 需求，企業內網資安面臨嚴重考驗

不只是個人資訊安全風險越來越高，企業面臨的資訊安全風險也同樣逐年高升。尤其在疫情發生後，企業內網的安全性受到了「在家工作」趨勢的嚴峻挑戰。
蔡松廷就指出，疫情後可以看到企業資訊安全可攻擊的面向增加，特別是因為員工必須在家上班，家中電腦的資安防護並未像企業內部電腦這麼高，加上頻繁使用 VPN，連線到企業內網的裝置大幅增加，使用的複雜度增加，對於公司內部負責網路裝置的人員來說，要判讀員工使用 VPN 是否造成異常的難度也大幅提升。
事實上，今年在疫情發生之後，就有許多企業與政府機關，因為 VPN 的使用，被駭客攻入內網造成資安的威脅。「從 VPN 找破口攻擊，就可以直搗核心，直接朝企業內網下手。」蔡松廷說。

一旦內網被入侵，包含公司員工的個人資訊、公司內部資訊，甚至是公司業務或技術研發技術資料都可能被盜、被鎖定或被威脅刪除。一位資安專家透露，今年不乏小型公司遭駭客鎖定勒索，更甚者是有同一間公司反覆被勒索。更糟糕的是，若內部資訊已遭駭客劫持，「大概只有付贖金才有機會拿回資料，或甚至拿不回資料」，專家不諱言。

今年光是企業遭到大型網路攻擊的案例就有好幾起，其中 Garmin 的案件因為涉及一般使用者，其嚴重性受到各界關注。Garmin 在今年 7 月傳出遭駭客攻擊，不但產線停工 2 天，連用戶的 App 都出現無法更新的狀況。甚至有傳言 Garmin 支付了 1,000 萬美元（約新台幣 2.9 億元）的「贖金」才解鎖攻擊。

除了 Garmin 之外，南韓企業 SK Hynix、LG 今年也都成為駭客攻擊目標，內部與客戶交易的機密資訊均遭曝光。儘管多數企業對於遭駭與贖金資訊三緘其口，但從一些調查結果中，也能一窺網路攻擊對企業帶來的危害有多嚴重。微軟就曾在 2018 亞太資安研究報告中指出，2017 年台灣由於網路資安攻擊事件而造成的經濟成本損失高達 270 億美元，換算成新台幣約 8,000 億元。

「資安即國安」只是口號？資安危機比你我想像的更嚴重

資訊安全危害不僅造成個人與企業損失，對於國家安全的侵害也成為政府的一大挑戰。對大部分民眾來說，「資安即國安」僅是一句常聽到的政府口號。然而，事實上，資安業內人士私下透露，我們的各個政府網站、醫療院所系統、智庫單位、媒體網站幾乎都是駭客鎖定攻擊目標，正是因為這些機構中有大量的全民個資與國家機密資訊。

甚至業者還提到，業內也有傳聞，來自中國的駭客正積極的蒐集台灣民眾的個資以及在社群平台上的資訊，用於中國政府情資分析，民眾在入境中國時的就可能因為自己曾在社群平台上的發言，或是親朋好友的動態而被盯上。也就是說，資訊安全的漏洞造成的除了經濟損失外，也會危及國民與國家的安全。

正是因為資安危害擴及範圍小至個人、大至企業、國家，而危機其實就淺藏在日常生活中的各種裝置中，往往只需要輕輕按下一個按鍵，就可能葬送個人的資訊，甚至是公司機密。也正是因為資安危機年年高升，《科技新報》特別規劃了系列專題，從個人、企業到法人與政府的角度來看資安風險，並進一步探討維護資訊安全更好的做法，以及台灣資安產業發展的潛能。