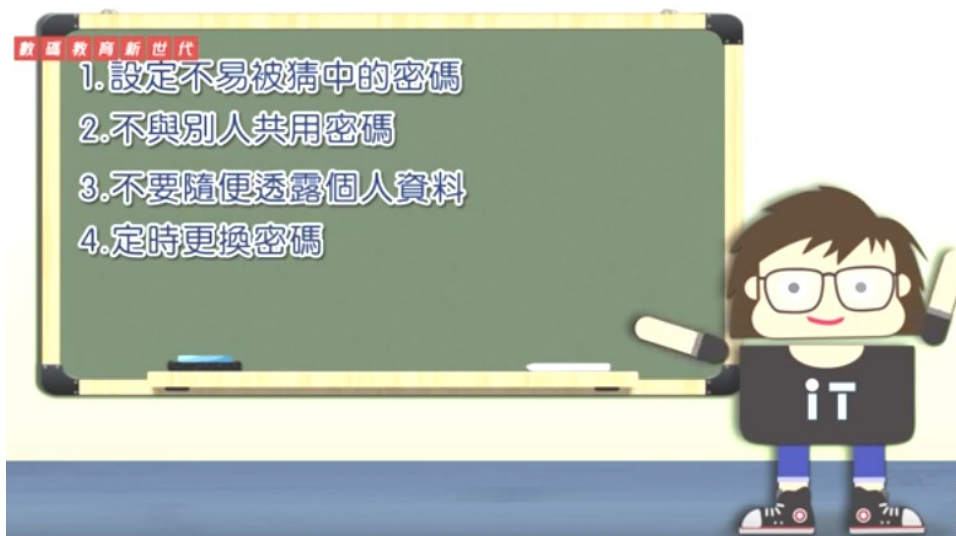




資訊安全維護

守護個資 保護隱私



資安時事案例

- ◎ 俄惡意軟體 VPNFilter 駭入 50 萬台以上路由器 知名大廠全遭殃
- ◎ 網美 IG 被盜遭勒索 駭客：給不雅照贖回

個人資料保護法

輕鬆學資安

- ◎ **WEP** (Wired Equivalent Privacy)

有線等效保密

數位學習

- ◎ 個人資料洩漏記

俄惡意軟體 VPNFilter 駭入 50 萬台以上路由器 知名大廠全遭殃

匯流新聞網記者藍立晴 / 綜合報導 2018 年 5 月 28 日

美 FBI 近日警告，俄羅斯駭客已入侵了 50 萬台家庭與辦公室路由器，可能蒐集用戶數據或直接癱瘓路由器，FBI 呼籲使用者將家中或辦公室的路由器並重新開機，下載更新檔案自我保護。

根據思科系統公司旗下的威脅情報組織 **Talos**，包括 Belkin International Linksys、MikroTik、Netgear、TP-Link 和 QNAP 等知名大廠的設備都在這波惡意軟體 VPNFilter 的攻擊名單內，這波針對路由器發動的攻擊相信是由俄國駭客集團 Sofacy（又稱 Fancy Bear 或 APT 28）所主導，目前已影響超過 54 個國家及地區，其中又以烏克蘭的情形最為嚴重。FBI 指出，由於攻擊手法相當複雜，此惡意軟體難以被察覺，敦促使用者立即重新啟動設備。

目前，**QNAP** 已為此作出回應，表示早在 2017 年就偵測到 VPNFilter，並在 2017 年中便釋出相關配套措施協助使用者偵測並移除 VPNFilter；**TP-Link** 則在官網中指出，強烈建議使用 TL-R600VPN 型號路由器的使用者更新設備韌體、關閉遠程管理功能。

Belkin International Linksys 則針對使用舊版路由器產品或路由器不支援自動更新的客戶於官網上釋出重啟裝置的**教學文**。Belkin International Linksys 同時澄清，新型的路由器如 Linksys mesh 或 EA/WRT 裝置並不會受到 VPNFilter 影響。

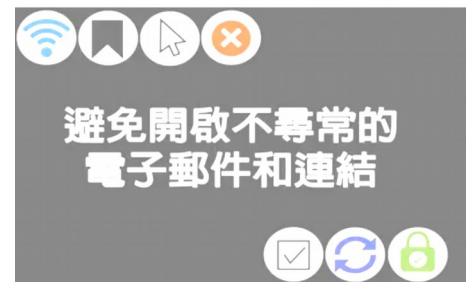
Netgear 在官網上強烈建議使用者更新至最新的韌體，並且更換默認使用者密碼、關閉遠程管理功能。

值得注意的是，今年 3 月初，德國才對 Fancy Bear 攻擊德國政府一事展開調查，根據調查結果，德國中央政府網路中的惡意軟體可能已存在長達一年的時間，2016 年美國民主黨全國委員會的伺服器亦曾遭到 Fancy Bear 滲入。



網美 IG 被盜遭勒索

駭客：給不雅照贖回



蘋果日報_2018 年 5 月 22 日

在社群網站《Instagram》上有 10 萬粉絲的網路正妹 Alice，經營了 6、7 年的帳號日前被盜，而該位土耳其駭客，還威脅她要拿錢出來回帳號，讓她感嘆「網路詐騙真的是一件很可怕的事情」。

Alice 在《臉書》粉絲團「愛麗絲的遊樂園」發文指出，她 20 日晚上 9 點多時，E-mail 信箱收到一封看起來是 Instagram 官方寄來的信件，於是就進去填了表格輸入了資料，回信之後查了一下這個藍勾勾的流程，突然驚覺是被騙了，這時要改 IG 的密碼已經來不及，已經被駭客登出且改掉帳號。

Alice 指出，駭客竄改她的帳號名稱，並且盜用她的帳號發文跟限時動態，感嘆網路詐騙真的是一件很可怕的事情，「駭客是土耳其人，應該是想要錢來威脅我，目前除了一直一直寫信之外不知道還能怎麼做」，也說這個帳號經營了六年，真的很希望能夠救回來。

Alice 接受《蘋果》訪問時提到，今天(22 日)早上駭客找到她的新帳號，並且跟她談條件，而對方發文內容為土耳其文，她用 Google 翻譯後得知，駭客要她的不雅照，不然就刪除帳號。Alice 強調，絕對不會理會駭客的要求，他們其實就是要勒索，不雅照之後就是要錢，目前不敢驚動駭客的原因，也是帳號經營了 6 年，大大小小的回憶都在裡面，怕駭客一不開心就把東西整個刪掉，所以才新開一個帳號進行連署，希望能夠將帳號救回來。(即時新聞中心／綜合報導)



公務機關因個人需要，想利用個人資料，應注意或遵行何種規定？



資料來源：花蓮縣政府

- 一、個人之醫療、基因、性生活、健康檢查及犯罪前科資料不得蒐集。
- 二、應於執行法定職務必要範圍內，且與蒐集的特定目的相符。
- 三、但有下列任一情形者，仍得利用：
 - 1、法律明文規定。
 - 2、為維護國家安全或增進公共利益。
 - 3、為免除當事人之生命、身體、自由或為防止他人權益之重大危害。
 - 4、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要者。





資料出處：行政院國家資通安全會報技術服務中心

WEP 是 Wi-Fi (無線相容性認證) 網路的基本安全功能，能將訊息以 40 位元和 128 位元的加密方式譯成密文透過無線網路傳輸。惟 WEP 已被證實可輕易被破解，有很多工具可以自由地截取加密訊息並在十分鐘裡破解你的 WEP 金鑰。故建議使用其他加密措施來取代 WEP 的使用；雖然如此，若無其他選擇，使用 WEP 總比完全沒有任何加密措施要來得好。

