公務機密維護宣導

如何避免駭客入侵

73%的網路用戶都曾是網路犯罪(如駭客攻擊) 的受害者。

寄發電子郵件、在臉書塗鴉牆上更新訊息、進入網路銀行查詢帳戶餘額……但凡您在網路上的一舉一動，都可能面臨駭客入侵的危險。

近年，知名科技雜誌《連線》的資深撰稿人麥特．霍南就慘遭駭客攻擊，儲存在手機、平板電腦和筆記型電腦裏的資料全都遺失，包括他一歲女兒的相片。為此，他在《連線》雜誌上寫道：「我整個數位生活毀於一旦！」然而以他的背景，理當對駭客的潛在危險瞭若指掌才對。

以下提供五個小訣竅，能降低您被「駭」的風險，免得您成了新一代反電子產品的極端份子。

1.留意分享的資訊

不必為了安全性而關閉臉書或推特帳號，但請牢記：但凡在社羣網站公開出生年月日、畢業日期、母方姓氏等資訊，都等於是在幫駭客一把，這些都是進入電話或網路帳戶時回答認證問題的重要資訊。

2.選擇複雜難解的密碼

如果您的密碼是由六個小寫字母組成，駭客的電腦可能只需十分鐘就能破解。現在有許多免費的網站(如 safepasswd.com)，可以組合大寫字母、符號與數字，創造出幾乎無法破解的密碼。另外，用一組字詞作密碼也是不錯的選擇 (可參考網站 passphra.se)。比如以「say no to hackers」(「向駭客說不」)為密碼，理論上，駭客得花幾千年的時間才能破解──至少目前而言是如此。

3.設定雙重認證程式

臉書和 Gmail 都有雙重驗證設定的選項，一旦啟用，登入時都必須輸入兩組密碼：自己原先設定的密碼，再加上以簡訊方式傳送給用戶的認證碼。網路科技媒體 CNET 寫手麥特．艾略特表示：「增加步驟多少會造成不便，但兩害相權取其輕，相較於被駭的風險，這麻煩還是值得。」Gmail 要設定這種「兩步驟驗證」，請進入「設定」後依序點選「帳戶」、「其他 Google 帳戶設定」、「安全性」，就可以進行兩步驟驗證。至於臉書，則要先登入自己的帳戶，點選位於「首頁」的「帳號設定」，再選擇「帳號保全」，最後進入「登入許可」。

4.謹慎使用 Wi-Fi

許多公共場所，如咖啡廳、機場和旅館都可以使用免費 Wi-Fi，但這類免費網路不見得會對筆電和網路之間所傳輸的資料加密。這意味使用者的電子郵件密碼、銀行帳戶餘額等資訊完全暴露在駭客威脅之中。用完免費 Wi-Fi 後，記得要斷線。方法如下：在微軟的視窗作業系統中，以滑鼠右鍵點擊工具列上的無線網路標示；在蘋果電腦的系統中，則點工具列中的 Wi-Fi 圖示。

5.備份資料

駭客能在幾分鐘內就把您珍藏多年的電子郵件、相片、文件、音樂等檔案從電腦中悉數刪除。如果您是蘋果用戶，不妨將電影、音樂和相片存放到雲端硬碟 iCloud 上，安全性相對較高。此外，也可以從 crashplan.com 和 dropbox.com 等網站下載簡單的備份系統來保護個人的數位檔案。

如果發生下列情況，代表您可能已經被駭：

- 登入電腦、電子郵件信箱或臉書等網站時，輸入平常使用正確無誤的帳號密碼卻登入失敗。
- 桌上型電腦桌面看起來有點不同，或是瀏覽器的首頁更換了。

- 電腦突然變得很慢，或經常受到彈出式的廣告騷擾。
- 朋友或同事說他們收到您的訊息，但您根本沒發出訊息。