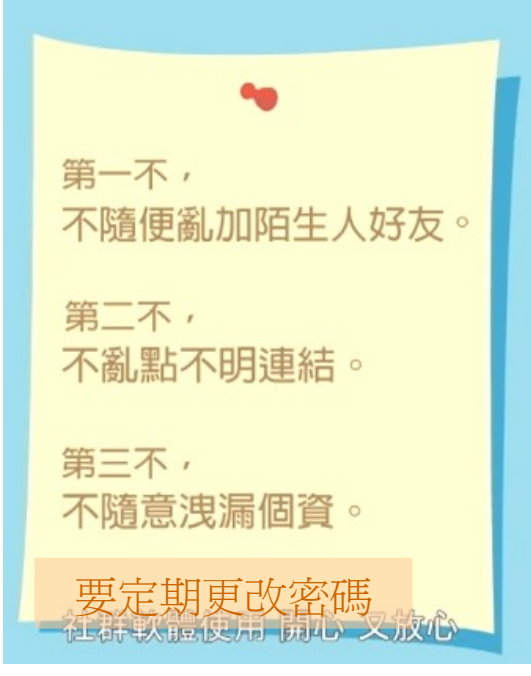
臺東林區管理處

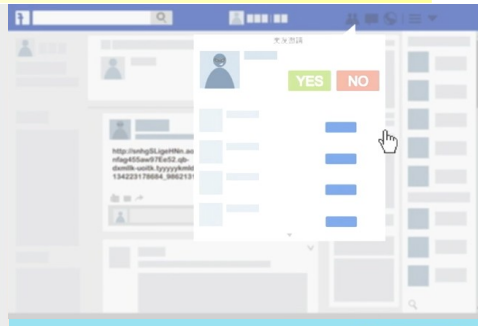
中華民國 106 年_ 11 月號

別輕易洩露個人資料



避免自己受到資訊安全的威脅

記住 3 不 1 要



資安時事案例

免費 WIFI 真的安全嗎？　5 招教你遠離駭客攻擊

你的網路個資 成駭客金庫

個人資料保護法　Q&A

輕鬆學資安

Stealth viru 隱形病毒

數位學習　104 年資安動畫金像獎

一分鐘看懂資安

免費 WIFI 真的安全嗎？　5 招教你遠離駭客攻擊

今日新聞 NOWNEWS 生活中心 台北報導

隨著現代人對網路的需求增加，許多公共場所、運輸工具都會提供免費 Wi-Fi 上網，不過用了真的安全嗎？

資安業者趨勢科技指出，不論是開放或私人 Wi-Fi ，駭客其實都有辦法連到你正在使用的網路，只要取得一小部分存取權限就能透過網路上現成的工具查看你的流覽內容，並從中取得你的電子信箱內容、通訊軟體內容等資訊，尤其在連線後掛網或使用免費 Wi-Fi 時，更會讓駭客有機會入侵。

爲此，趨勢科技提供五大方法遠離駭客攻擊：

1. 不時確保手機系統是最新版本，舊版遭受駭客入侵機率往往比新版高。
2. 使用完 Wi-Fi 網路後，一定要記得登出，保持連線會提供駭客大量入侵用戶資訊的機會。
3. 若手機出現不正常的遲緩、當機、或冒出警告標語，切記趕緊中斷網路，這很可能是遭受大量惡意攻擊的前兆。
4. 確保下載程式的來源是可信任的，若是不明的來源盡量不要下載，才不會容易把惡意軟體連同應用程式帶進你的行動裝置。
5. 盡量避免連接免費的 Wi-Fi 網路，若大量使用免費 Wi-Fi ，這也表示你大量曝光在駭客眼前，成爲下個入侵目標的機率也更大。

HOME

你的網路個資 成駭客金庫

2017-10-21 00:20 經濟日報 編譯／廖玉玲

你的網路個資值多少？你可能覺得是無價之寶，對駭客而言呢？你可能會很意外，甚至覺得「被侮辱」。

根據戴爾旗下資安公司 Secureworks 的最新年度調查，美國、日本和南韓等國驗證過且額度高的信用卡，在「黑暗網路」（ dark web ，暗網）裡，一張大約價值 10 到 20 美元。

Secureworks 對「暗網」的定義是「網路論壇、數位商店和聊天室等的集合，網路罪犯會在這裡結交狐群狗黨、交易工具和技術、以及兜售駭得的資料，包括銀行資料、可辨識的個人資料等內容」。

Secureworks 資深安全研究員堤里指出，現在信用卡在暗網已經不便宜了，但買家比較能買到「較優質」的卡。目前以企業卡和高額度的個人信用卡最受歡迎，一張約 15 至 20 美元，一張萬事達卡的普通卡大概只值 9 美元。

而平凡如你我的個人資料，在地下網路市場也有行情，包含姓名、地址、信用卡資料、社會保險號碼和出生日期等的「 Fullz 」套餐資料，最低 10 美元就能買到。這類資訊能協助詐騙者繞過許多網路交易時需要回答的「秘密問題」（ secret question ）。

可用來僞造報稅資料的文件，行情就很不錯了，根據 IBM 資安研究集團 IBM X-Force 今年稍早提出的報告，尚未過期的報稅資料，一份可以賣到 40 甚至 50 美元。堤里提醒，沒有任何個資是「無害」的，犯罪者會收集大量個資，然後一直等到某個時機拿來使用。

堤里說，每樣東西都非常珍貴，即便只有一點點資訊，「卻也可能是某個想冒用你的名字去貸款的歹徒一直湊不齊的最後一片拼圖。你不知道這些罪犯有多大本事，但等到知道了也就來不及」。堤里也說，信用監測和凍結，可能是自我保護的唯一希望，「問題在於你非常放心地把資料交給第三方公司保管，情況就變得不是你能掌握的」。

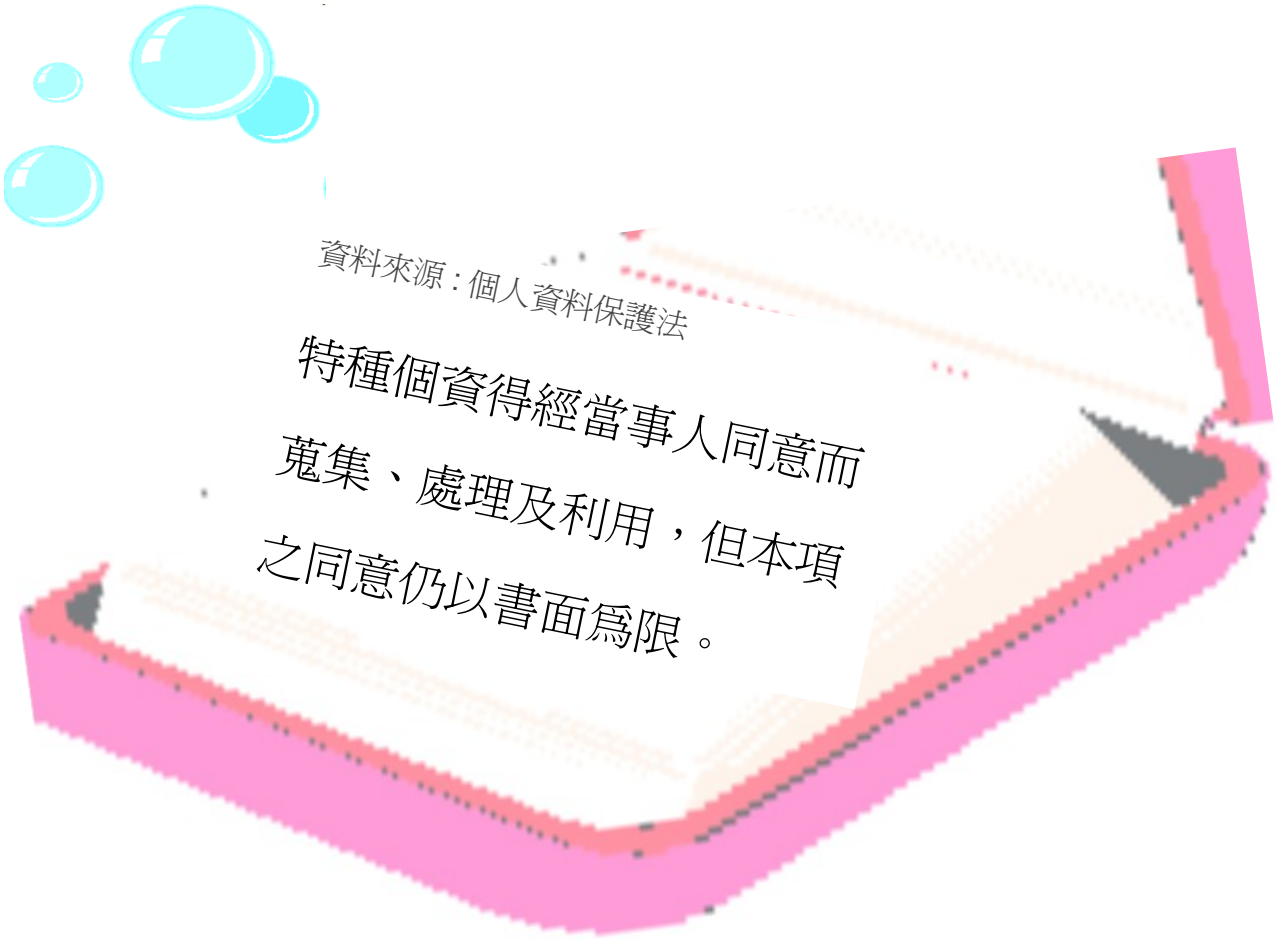
駭客要兜售這些竊取來的資料時，主要是透過一種稱爲 Tor 的特殊軟體，連結上暗網的網站，一般的網路用戶大多不會連上這類網站。對於兜售毒品及駭來的個資等不合法的經濟活動而言，這些網站就是他們的通路。

另外值得注意的是，在暗網上交易的不只是個資，有些賣家也會教願意付費的客戶如何使用這些個資，以進行稅務詐騙或開假帳戶等非法行爲。對於那些技術層次較低的客戶，有些賣家會指點他們如何利用臉書、 Instagram 或推特等在「表層網路」就有的社群媒體，收集到生日、生平小故事等部分資訊，冒名申請假帳號時就很好用了。

專家一再呼籲，應該至少要更換密碼一次，且絕對不要重複使用同一組密碼，這樣歹徒就算找到你的帳號也無法使用。

HOME

最近一次個資法修正後，關於「同意」的新法則爲何？



HOME

Stealth viru 隱形病毒

資料出處： iThome

這是一種會嘗試躲避偵測的病毒，該病毒發作後，會立即將自身病毒體刪除，然後將病毒碼插入到正常的系統文件中以躲避防毒軟體的偵測，讓電腦以爲沒有中毒，卻由已遭受感染的區域散佈病毒。