2023資訊安全宣導課程

林彥丞 112/11/15

大綱

- 何謂資訊安全
- 個資與資安事件案例分享
- 社群網路常見詐騙方式
- 常見的攻擊手法
- 資訊安全發展趨勢與新興議題
- 社群網路安全使用守則
- 常見電腦遭入侵「跡象」與「應對」

何謂資訊安全？

攻擊者的動機因人而異，取決於其個人或組織的目標、價值觀、利益和背景。以下是一些可能的攻擊者動機：

1. 經濟動機：
2. 政治或社會動機：
3. 情報收集：
4. 敵意或報復：
5. 挑戰和樂趣：
6. 惡意行為：
7. 商業競爭：

攻擊者的動機的多樣性意味著需要針對不同的情境實施多層次的安全措施，以應對各種可能的威脅。企業和組織應該不斷更新其安全政策和實踐，以確保能夠有效地應對不同動機的攻擊。

何謂資訊安全？使用者為什麼成為目標?

使用者成為攻擊的目標的原因多種多樣，攻擊者可能針對個人使用者或組織內的員工。以下是一些可能的原因：

1. 資訊收集：
2. 金融盜竊：
3. 身份盜竊
4. 企業間諜活動：
5. 社交工程勒索：
6. 電子郵件和網路釣魚：
7. 雇主攻擊：

為了保護自己，使用者應該保持警覺，遵循良好的網路安全實踐，包括使用強密碼、定期更改密碼、不點擊不明連結、不隨意提供個人信息等。組織應該提供安全培訓，以教育員工辨識和應對各種網路攻擊。

何謂資訊安全？

資訊安全（Information Security）指的是保護資訊免於遭受未經授權的存取、損害、變更、洩漏或破壞的一系列措施和技術。這包括確保資訊的機密性、完整性和可用性，以及防止未經授權的存取、使用、公開或毀損。
資訊安全的目標包括：

1.機密性（Confidentiality）：
2.完整性（Integrity）：
3.可用性（Availability）：
4.身份認證（Authentication）：
5.授權（Authorization）：
6.非否認性（Non-repudiation）：

資訊安全的實踐包括使用加密技術、設立防火牆、實施存取控制、進行風險評估和管理、定期進行安全審查和監控等。這是一個不斷演進的領域，因為科技的進步和新的威脅不斷湧現，組織需要不斷調整和改進其資訊安全策略和措施。

個資與資安事件案例分享

個資與資安事件案例分享

個資與資安事件案例分享

資料來源：華視 https://news.cts.com.tw/cts/life/202212/202212062118012.html

個資與資安事件案例分享

資料來源：https://www.cardu.com.tw/news/detail.php?45862

個資與資安事件案例分享

資料來源：https://www.ithome.com.tw/news/152491

個資與資安事件案例分享

資料來源：https://youtu.be/jhlMveZuYeo

個資與資安事件案例分享

資料來源：https://ctee.com.tw/news/stocks/669490.html

個資與資安事件案例分享

資料來源：https://ec.ltn.com.tw/article/breakingnews/4139451

個資與資安事件案例分享

資料來源：https://news.ltn.com.tw/news/life/breakingnews/4147163

個資與資安事件案例分享

資料來源：https://news.ltn.com.tw/news/society/breakingnews/4180017

個資與資安事件案例分享

資料來源：https://www.businesstoday.com.tw/article/category/183027/post/202302150040/

個資與資安事件案例分享

資料來源：https://udn.com/news/story/123309/6989196

個資與資安事件案例分享

2022年10月21日，以「OKE」為代號的匿名使用者，在駭客論壇BreachForums兜售號稱全台2300 萬筆戶役政資料。為了吸引顧客買單，OKE更直接公開20萬筆設籍在宜蘭的個資當作商品樣本。

其中包含39個欄位，從個人生日、 性別、身分證號等資訊外，戶號、 戶□，甚至是生父生母、養父養母 都有單獨欄位和對應的身分證號。

資料來源： 天下雜誌

個資與資安事件案例分享

資料來源： https://news.cts.com.tw/cts/general/202303/202303312160730.html

個資與資安事件案例分享

資料來源： https://udn.com/news/story/6885/7166514

個資與資安事件案例分享

資料來源： https://today.line.me/tw/v2/article/RBy9Pae

個資與資安事件案例分享

資料來源： https://ec.ltn.com.tw/article/breakingnews/4318169

個資與資安事件案例分享

資料來源： https://www.ettoday.net/news/20230517/2500933.htm

個資法修法三讀通過

資料來源： https://www.ndc.gov.tw/nc_27_36901

台灣成駭客天堂

一名駭客和某不具名政府資安顧問不約而同私下透露，駭客正在暗網上，散布華航第二波個資名單，包括新任民進黨智庫「新境界文教基金會」副董事長童子賢、名人孫芸芸、藝人蔡依林，近日已被陸續洩漏個資、兜售。

資料來源：https://vip.udn.com/vip/story/121938/6951115

台灣成駭客天堂

資料來源：https://topic.udn.com/event/newmedia_hacker_taiwan

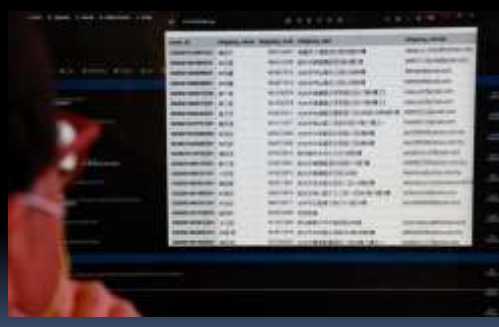
台灣成駭客天堂

資料來源：https://topic.udn.com/event/newmedia_hacker_taiwan

台灣成駭客天堂

資料來源：https://topic.udn.com/event/newmedia_hacker_taiwan

台灣成駭客天堂

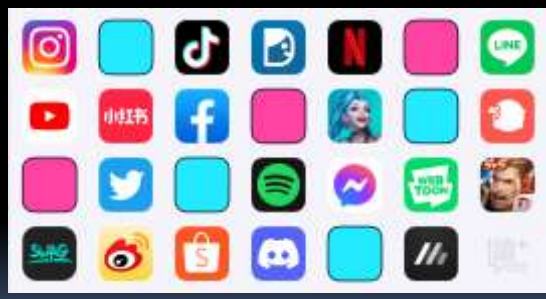


資料來源：https://topic.udn.com/event/newmedia_hacker_taiwan

台灣成駭客天堂

資料來源：https://topic.udn.com/event/newmedia_hacker_taiwan

社群網路常見詐騙方式



台灣年輕人間爆紅的「小紅書」是什麼？

- 「小紅書」是中國知名的「網路購物」和「社交APP」，人稱「中國版的IG」。電商可PO文，一般人也能分享「好物」。
- 操作與IG差不多，可發文(小紅書稱為筆記)、限時動態(小紅書稱發佈瞬間)、介面也是圖片影音為主，亦有按讚、分享、留言等基本社群功能。
- 可分享美妝、穿搭；也能紀錄生活大小事。可透過「標籤」將自己包裝成網紅。
- 小紅書是中國時下少女追蹤流行資訊必備的搜尋平台。
- 不少人把小紅書當成Google、百度等搜尋引擎。
- 購物或潮流相關問題都先使用小紅書搜尋，或直接使用APP內的「商城」購買商品。
- 台灣00後妹子笑「IG是老阿姨玩的」！
- 很多年輕人都改用小紅書。

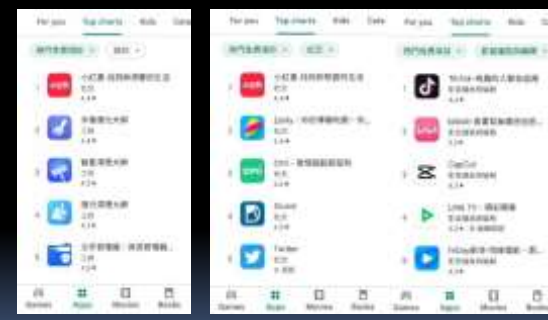
資料來源：風傳媒

臉書、IG落伍了？這2款App稱霸Google Play熱門排行

- 《READr讀+》曾針對學生族群最喜愛的社交軟體進行調查，國高中生最愛的前三名分別為IG、FB與TikTok，小紅書排第6名，而大學生最愛IG、FB與Dcard，小紅書排名第10，這份問卷的採樣時間為2020年12月30日至2021年4月26日，但隨著小紅書的知名度越來越高，它的排名似乎也出現了改變。
- 根據Google Play的熱門免費項目排行，小紅書同時囊括「社交」類與「所有類別」的冠軍，其他熱門社交App分別為Twitter排名第5、Instagram排名第6、Facebook排名第9，而「TikTok」則是「影音播放與編輯」類的第一名，「所有類別」則排名第11。
- 當時網友發文表示，現在年輕人都改用中國知名社交App小紅書，是不是沒玩小紅書就落伍了？雖然有網友擔心會有文化統戰的問題，但也有人認為，小紅書相當實用，資訊的完整度勝過IG。

資料來源： https://www.storm.mg/lifestyle/4195441

小紅書、TikTok 排行



資料來源： https://www.storm.mg/lifestyle/4195441

「小紅書」爆紅原因？與IG差在哪裡？

有「中國版Instagram」之稱的小紅書，有著與Instagram相似功能如：以圖和影音為主的介面呈現、發佈瞬間豐富濾鏡(類似IG story)、發文私訊按讚分享等社群功能。然它與Instagram較不同的功能是：

1. 新註冊用戶可依興趣選擇喜好內容
2. 推薦貼文不侷限於單一主題，能自動延伸相似內容
3. 演算法自動推送貼文至手機通知欄
4. 內建熱門音樂庫、精美影集模板，讓用戶直接套用
5. 以「教程」為主的影片內容，網紅專家一分鐘內「包教包會」
6. 素人即網紅：粉絲翻漲容易，因標籤會自動推應相似主題，易被看見
7. 廠商利用網紅打造「商城」利益

資料來源： https://www.storm.mg/lifestyle/3443657?mode=whole

網路上的假訊息

網路上的假訊息是指故意製造、散布虛假或誤導性信息的行為。這樣的信息可能是在社交媒體、新聞網站、論壇等網路平台上流傳，目的往往是影響公眾觀點、製造混淆、引起恐慌、操縱選民情緒、破壞特定組織或個人的聲譽，甚至可能是出於娛樂目的。

以下是一些假訊息的定義和可能的目的：

1.定義：
   1. 虛假信息：
   2. 誤導性信息：
   3. 未經證實信息：

2.目的：
   1. 影響公眾觀點：
   2. 政治操縱：
   3. 創造恐慌：
   4. 增加點擊率：
   5. 商業競爭：
   6. 娛樂：

假訊息的流通可能會對社會、政治和經濟產生負面影響，因此應該加強人們的媒體素養，提高對假訊息的辨識能力，同時推動社交媒體平台、新聞機構和政府等各方合作，以應對這一問題。

假消息的特徵

1. 太過於誇張、聳動、讓人不禁想點擊的標題
2. 網址很可疑，即可能是假冒的新聞網站
3. 新聞內容出現許多錯字或網站版面編排不正常
4. 很多明顯經過刻意修圖的照片或圖片
5. 沒有附註發布日期
6. 未註明作者、消息來源或相關資料

資料來源：https://www.storm.mg/lifestyle/3443657?mode=whole

要避免成為假消息的受害者和傳播者

您可以採取以下一些建議：

1.驗證消息來源：
2.交叉驗證信息：
3.留意模糊或不確定的信息：
4.謹慎對待社交媒體信息：
5.確保消息與常識一致：
6.注意號稱專家的信息：
7.不要隨意轉發或分享：
8.參與教育和媒體素養培訓：
9.使用事實查核工具：
10.保持冷靜和理性：

這些建議有助於保護您免受假消息的影響，同時也有助於減少您成為虛假信息的傳播者。

訊息辯真偽

收到可疑訊息(新聞、郵件、簡訊...等)，可至『Cofacts 真的假的』網站 查詢訊息的真偽。

- **網址**：https://cofacts.tw/
- **Facebook**：https://zh-tw.facebook.com/cofacts.tw/

常見的攻擊手法

什麼是駭客攻擊？
您可以把網際網路想像成一條帶領您通往目的地的路線，路線中的每個連結都是資訊在到達目的地和返回途中的必經之處。駭客攻擊常被定義為利用漏洞和 Bug 入侵電腦系統，並存取機密資料。駭客會使用合法（如安全研究）和非法（如憑證盜竊、勒索軟體）手段進行入侵。

簡言之，駭客經由尋找路線上任何連結中的弱點進行入侵，如果他們找到一個弱點，就能進行攻擊並造成嚴重破壞。

資料來源：https://nordvpn.com/zh-tw/blog/heike-gongji/

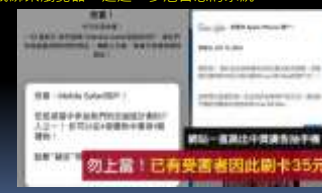
常見的攻擊手法

假冒無線熱點（Fake WAP）
這是一種非常簡單的駭客攻擊，很容易吸引受害者。飯店、咖啡廳或機場等公共場所的免費 Wi-Fi 熱點不一定安全，因為駭客可能會偽造這些場所的 Wi-Fi 熱點名稱，引誘人們連線。當有人連上這些假冒的 Wi-Fi 熱點後，駭客就能監控他們的網路活動，竊取機密資料，甚至強迫在設備上安裝惡意程式。

資料來源：https://nordvpn.com/zh-tw/blog/heike-gongji/

常見的攻擊手法

網頁偷換行為（Bait & Switch）
這種網路詐欺行為也稱為誘餌行為，它使用「廣告」這種吸引人們點擊的途徑，欺騙用戶進入惡意網站。Facebook 和 Google 這些大型廣告商已經建置一系列防護措施來避免這種行為，但仍無法保證駭客不會經由這種方式進行攻擊。當您點擊廣告之後，駭客就能使用許多其他的攻擊手法，例如下載惡意程式、點擊劫持（clickjacking）或綁架瀏覽器，進進一步危害您的系統。



資料來源：https://nordvpn.com/zh-tw/blog/heike-gongji/

常見的攻擊手法

帳號填充攻擊（Credential reuse）
這種攻擊是攻擊者透過遭駭網站所流出的帳號資料，嘗試使用這些帳號資料登入其他服務。當駭客利用系統漏洞取得某個網站的用戶帳號資訊，或者尋找已遭外洩的網站帳號資料庫後，就能利用這些帳號嘗試在其他網站上進行登入，以獲取其他網站上更多的機密資料。
因此，不要在所有網站上都使用相同的密碼，以確保其他帳戶的安全。如果發現某個網站有帳號外流的新聞，請盡快更改該網站的密碼。

資料來源：https://nordvpn.com/zh-tw/blog/heike-gongji/

常見的攻擊手法

SQL 注入式攻擊（SQL injection）
SQL 注入式攻擊又稱 SQL 資料隱碼攻擊，是一種常見且強大的駭客攻擊手法，也是一種非常不安全的網站漏洞。某些系統在建置時產生的漏洞，使得駭客可以在網頁上的輸入欄位插入 SQL 語法，讓系統運行這段SQL語法。

資料來源：https://nordvpn.com/zh-tw/blog/heike-gongji/

常見的攻擊手法

瀏覽器綁架
瀏覽器綁架是一種常見的駭客攻擊手法，被攻擊的對象通常不是很懂技術。在引導用戶進入惡意網站或感染合法網站之後，駭客會建立一個佔據螢幕的彈出視窗，或者被安裝根本用不到的工具列。這個視窗或工具列難以移除或無法關閉，視窗上通常會顯示防毒軟體的警告或其他詐騙訊息，並指示用戶打開偽造的技術支援連結，讓用戶在不知不覺中付錢給駭客。

資料來源：https://nordvpn.com/zh-tw/blog/heike-gongji/

常見的攻擊手法

網路釣魚（Phishing）
與大多數駭客攻擊不同，網路釣魚的目標是設備的用戶，而不是設備本身。這種攻擊經由一封精心設計的電子郵件來欺騙受害者，誘導受害者打開郵件上的惡意網站連結或郵件上的附件，讓受害者的設備受到感染，進而竊取設備上的機密資訊。
網路釣魚有非常多的攻擊手法，其特徵是偽裝成來自可信任來源的郵件或訊息，誘騙受害者上當。最簡單的預防方法是對電子郵件保持懷疑的態度，如果一封看起來正常的電子郵件附帶可疑的連結，請檢查網址的正確性。也不要隨意開啟電子郵件上的附件，除非您確定附件是安全的。

資料來源：https://nordvpn.com/zh-tw/blog/heike-gongji/

常見的攻擊手法

點擊劫持（Clickjacking）/介面偽裝（UI redress）
許多用戶可能在瀏覽網站時，沒有注意到它其實是惡意網站，或者是合法網站被入侵後成為惡意網站。這些網站看似正常的網頁上，隱藏著看不見的框架或按鈕，引誘用戶點擊或誤觸，有些攻擊甚至可以追蹤用戶的滑鼠和鍵盤行為。用戶執行的任何一次點擊都是在執行某種他們不知道的動作。

資料來源：https://nordvpn.com/zh-tw/blog/heike-gongji/

常見的攻擊手法

蠻力攻擊（Brute force）
在蠻力攻擊中，駭客嘗試猜測密碼、PIN 碼或加密金鑰。駭客透過這種攻擊手法，可以存取受保護的服務和資料庫，或者解密資料。用戶也可以因為安全原因使用蠻力破解來測試自己的密碼安全強度。
駭客使用的軟體每秒會嘗試大量密碼組合，直到猜測正確密碼為止。因此，如果您的密碼規則很簡單，這類軟體只要幾秒就能破解密碼。然而，破解複雜密碼則需要幾年的時間。

資料來源：https://nordvpn.com/zh-tw/blog/heike-gongji/

常見的攻擊手法

結論

養成良好的習慣，例如不要隨意打開來路不明的連結、加強密碼強度、更新或升級為更安全的作業系統、上網時使用 VPN 等，都有助於避免遭駭客攻擊。

此外，網路上有各種不同的漏洞和網路犯罪手法，儘管無法全部都了解，然而學習上述的常見駭客攻擊技術，應該會對網路安全有所幫助。一般來說，您不需要瞭解和識別所有的攻擊手法，但必須有足夠的知識對常見的駭客手法進行防禦。如果您瞭解這些常見的駭客攻擊方法，就能事先準備阻擋和防禦駭客的攻擊。

資料來源：https://nordvpn.com/zh-tw/blog/heike-gongji/

全球資通安全威脅趨勢

全球資通安全威脅可以分為多個類別，以下列舉了六大主要類別：

1.釣魚攻擊（Phishing Attacks）：
2.勒索軟體（Ransomware）：
3.零日漏洞利用：
4.物聯網（IoT）安全威脅：
5.社交工程攻擊：
6.供應鏈攻擊：

這些威脅類別之間可能存在重疊，而且隨著科技和攻擊手法的演變，新的威脅類別也可能不斷出現。因此，資通安全專業人員和組織需要持續關注和應對不斷變化的威脅環境。

政府領域資安威脅趨勢

政府領域的資安威脅可以從不同面向來分析。以下是政府領域資安威脅的六大主要面向：

1.資料安全：
2.網路安全：
3.身份和訪問管理：
4.基礎設施安全：
5.社交工程和資安文化：
6.國際和地緣政治風險：

社群軟體安全最佳守則

1.強化密碼安全性：
2.啟用雙重認證 (2FA)：
3.定期檢查隱私設定：
4.警惕釣魚攻擊：
5.定期更新軟體：
6.謹慎分享個人資訊：
7.避免使用公共電腦：
8.訓練員工和社區成員：
9.監控帳戶活動：
10.報告問題：

即時通訊軟體注意事項(1)

- 不得於公務個人電腦安裝
- 以傳送溝通訊息為主
- 傳遞訊息，內容不得涉及機密性、 安全性、隱私性或洩漏個人資料
- 機關聯絡群組，指定管理人員
- 管理人員應建立群組名冊並定期清 查群組成員，每月將群組訊息內容


即時通訊軟體注意事項(2)

- 機關交付正式文書，應循現有行政程序辦理(例如:公文、E-mail)
- 管理員應適時向群組成員宣達使用注意事項，發現問題應立即處理。成立群組目的消失，應即時刪除。
- 群組成員發現誤傳或內容不當者，應即時主動通報管理員處置


電腦安全

- 長時間離開辦公室，記得將電腦關機
  - 杜絕來自網路破壞
  - 防止帳號或密碼被盜用
  - 防止重要資料遭竊
- 應用程式不用時，登出應用程式及作業系統
- 離開座位，電腦應該設定螢幕保護程式
- 辦公室電腦不得任意加裝與工作無關之軟體

機密資料保護

- 紙本
  - 機密及敏感文件不可遺留於桌面上，必須存放於安全場所並加以上鎖
  - 作廢、敏感文件不得回收再利用
- 電子資料
  - 重要或敏感檔案要分開存放
  - 設定密碼或以加密軟體保
  - 建議避免共用資料夾

重要資料備份

- 備份的重要性
  - 預防重要資料或設備損壞遺失
  - 確保可用性
  - 防範勒索病毒
- 可藉由以下方式達到備份目的
  - 不同的儲存媒體
  - 各式各樣的工具軟體
  - Windows本身所提供的程式
  - 網路存放及備份(加密上傳)

常見電腦遭入侵「跡象」與「應對」

如果不想成為網路犯罪的受害者，請留意以下十個跡象，代表您的電腦設備可能已被駭客入侵：

1. 您收到勒索軟體訊息
2. 電腦跑很慢
3. 視訊鏡頭自行開啟
4. 您的朋友收到來自您電子信箱不明郵件
5. 頻繁的出現彈跳視窗
6. 工具列突然出現新圖標
7. 出現隨機圖標
8. 密碼無法使用/無法登入
9. 個資和帳號資訊在暗網流通
10. 防毒軟體的警告

資料來源： https://version-2.com.tw/

常見電腦遭入侵「跡象」與「應對」

1.您收到勒索軟體訊息

最顯而易見的是，當您開機時不是出現一般的啟動畫面，而是看到勒索訊息，那麼您很有可能已成為勒索軟體的受害者了，它通常會給一個很短的支付時限及說明如何支付贖金，但不幸的是，即便您確實遵守了指示，也有三分之一的機會無法重新獲得這些加密文件的存取權限。

2.電腦跑很慢

當惡意軟體（包括特洛伊木馬、蠕蟲和加密貨幣挖礦）植入於電腦設備時，它們通常會使運行變慢，尤其是加密劫持攻擊，它會佔用大量的效能，當然電腦跑很慢不全然是惡意因素所造成，也有可能是電腦設定不佳等問題。

資料來源： https://version-2.com.tw/

常見電腦遭入侵「跡象」與「應對」

3.視訊鏡頭自行開啟

駭客使用的一些間諜軟體除了可以取得您在電腦設備的資料外，還能偷偷打開視訊鏡頭和麥克風，藉由這樣記錄和竊取您和您家人的視頻，進而用於勒索，所以請密切留意視訊鏡頭，檢查它是否會自行開啟，ESET資安專家建議最好利用貼布貼住，來確保不會使用到它。

4.您的朋友收到來自您電子信箱的不明郵件

還有一個證明您的電腦設備已被入侵的指標是，如果您的朋友和客戶開始收到來自您的不明電子郵件或社交媒體帳戶的垃圾郵件；典型的網路釣魚就是劫持受害者的帳戶，然後向他們的所有朋友發送垃圾郵件或網路釣魚。若所有帳戶都有使用雙重身份驗證(MFA)的機制，則可以輕鬆緩解這種威脅。

資料來源： https://version-2.com.tw/

常見電腦遭入侵「跡象」與「應對」

5. 頻繁地彈出視窗
廣告軟體通常透過受害者接觸過多的廣告量來讓攻擊者賺錢，因此，如果您的電腦頻繁地彈出式廣告，這代表某處可能安裝了一些惡意代碼或可能不需要的軟體。

6.工具列突然出現新的圖標
惡意軟體還可能在您的瀏覽器上安裝其他工具列，如果您發現任何您不認識或不記得下載的內容，則可能意味著您的電腦設備已被駭客入侵；如果您遇到 APT 團體的惡意軟體攻擊，則可能需要將您的電腦設備恢復至出廠設定才能將其刪除，若是PUA (Potentially Unwanted Application，潛在有害應用程式)的話，只要刪除應用程式和工具列就可以了。

資料來源： https://version-2.com.tw/

常見電腦遭入侵「跡象」與「應對」

7.出現隨機圖標
當惡意軟體安裝在受感染的電腦設備時，通常會出現新的桌面圖標，只要桌面整齊地排列成少量的文件、文件夾和程式，就可以輕易發現。ESET資安專家建議整理一下電腦桌面，以便更好地追踪電腦設備上的圖標。

8.密碼無法使用/無法登錄
如果駭客入侵了您的電腦設備，他們很有可能已經劫持了各種在線帳戶，例如您的電子郵件，並更改了密碼，將您拒之門外，這也是所有網路攻擊中最嚴重的情況之一。

資料來源： https://version-2.com.tw/

常見電腦遭入侵「跡象」與「應對」

9.個資和登錄資訊在暗網流通
如果您收到與您有業務往來公司之資料外洩通知，請務必嚴肅看待並在可以提供第三方確認任何違規行為，如HavelBeenPwned之類的網站進行驗證。另外利用暗網監控工具還可以在網路犯罪的相關論壇搜索您的資料，以更主動的方式來了解您的個資和登錄資訊之暗網流通狀況。還有若您能迅速進行更改密碼、凍結信用卡等行為，也可以降低被駭客利用或攻擊的風險。

10.您收到來自防毒軟體的警告
來自反惡意軟體工具的警告也應慎重看待，儘管耳聞有假冒的電腦防毒軟體彈跳視窗，但仍請確認訊息是否來自於您購買的電腦防毒軟體供應商，並按照說明嘗試查找並刪除您電腦設備上的惡意文件。

資料來源： https://version-2.com.tw/