# 一鍵風暴》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 8:37 | 分類 物聯網 , 社群 , 網路



專題

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。

---

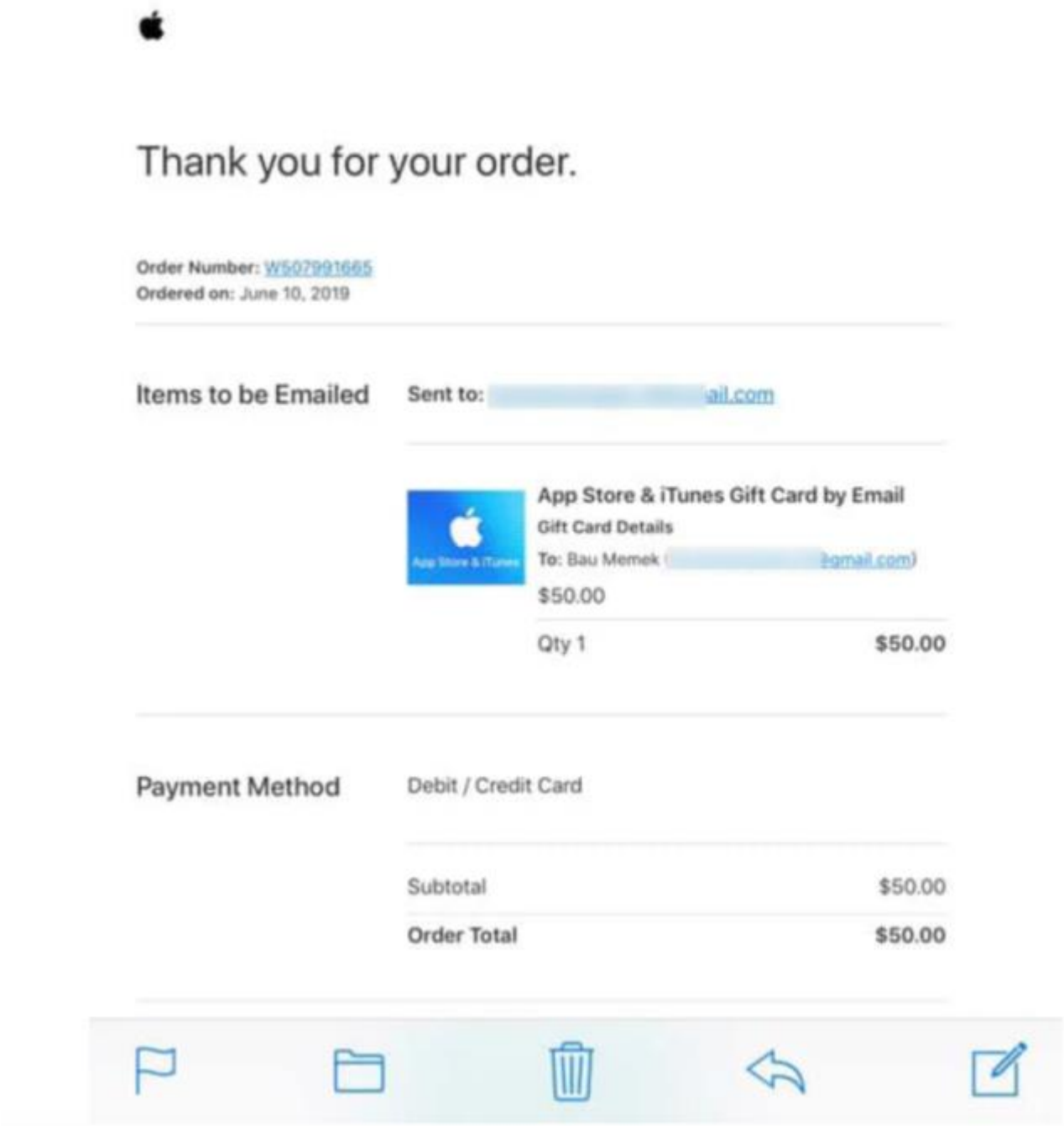
**我們離資安危機很遠嗎？再不小心！你的私密事就成全球共享資訊，只要輕輕點下一個按鈕，小至個人與家中訊息全被看光，大至整間公司的營業機密都可能跟著葬送。👉一鍵風暴資安系列專題》**

---

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。




▲ 網路釣魚信件偽裝成 App Store 訂單的 Email。

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。

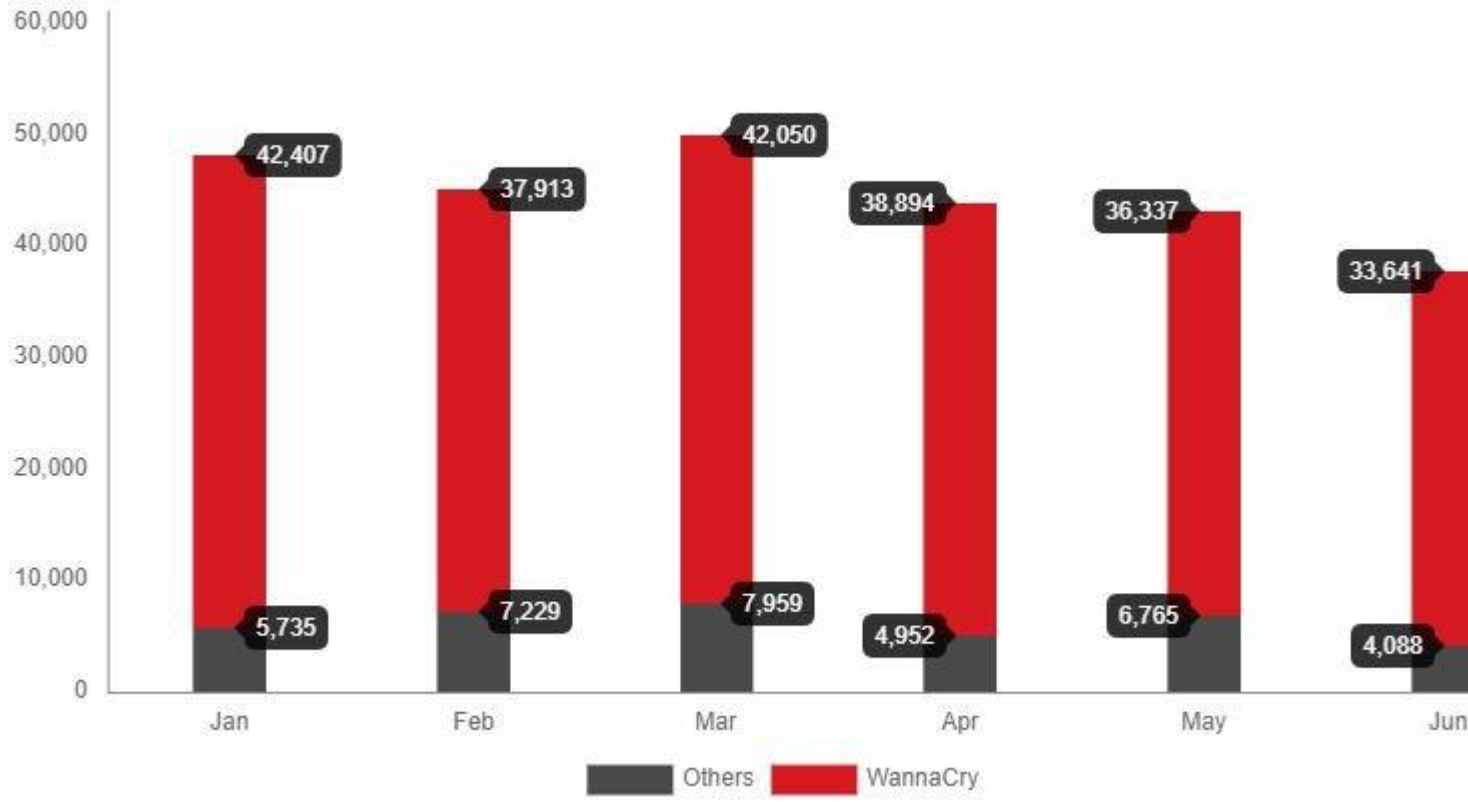

▲ 最好不要隨意連上來路不明的 Wi-Fi。

## 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）。




▲ WannaCry 仍占了絕大部分的勒索病毒偵測數量。

## 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。


▲ 詐騙訊息偽裝成中獎資訊易使民眾上當。

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贖金，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。

那麼，面對層出不窮的資安攻擊手法，民眾究竟該如何防範呢？對此，簡勝財提供了 9 項建議。

## 建議一：運用防毒軟體防範

這大概是最基本、也是一般人最常使用的方式。簡勝財表示，現今網路詐騙、網路釣魚已不限於單一詐騙手法，建議民眾至少要安裝防毒軟體，以有效偵測惡意網址及威脅。一旦點擊進入惡意連結，防毒軟體將會自動封鎖惡意網頁，在接觸到可疑詐騙網址前搶先予以攔阻，避免個資被竊，保護個資安全。


▲ 安裝防毒軟體有助偵測惡意程式或網址。

## 建議二：輸入帳密前再三確認是否為官方網站

當民眾遇到任何要求提供帳號資訊或是信用卡資訊的網站時，除了查明是否為正規的網站外，盡量不要使用對方提供的登入驗證連結。簡勝財建議，民眾遇到任何網址要求輸入帳號密碼或是號稱是「官方」的通知訊息時，請再三確認是否是官方網站，或是直接從官方網站登入查證。

## 建議三：嚴謹管理自己帳號

為了防止帳號被不當利用，建議民眾應該要因應不同的服務使用不同的帳號密碼；甚至若是能設定多重認證的話，請務必將此功能打開，可提升帳號安全度。

## 建議四：更新作業系統或是軟體修補或更新程式

民眾平時在收到電腦或智慧型手機作業系統（Windows、Mac、iOS 或 Android）和應用程式更新通知時應立刻進行更新，使其保持最新狀態，避免惡意軟體或惡意應用程式針對作業系統等安全漏洞進行攻擊。

## 建議五：不要任意安裝 App

在手機等行動裝置安裝各種 App 對一般人來說稀鬆平常，然而，簡勝財強調，智慧型手機或平板等行動裝置在安裝應用程式時，民眾必須慎重看清是否為非法應用程式再判斷安裝與否，並避免在非官方的應用程式商店下載 App。


▲ 有些 App 看似正常，但實際是惡意程式。

簡勝財提醒，在安裝應用程式前，可以確認應用程式及開發者的評價、評價數量等。此外，也要檢查應用程式的許可權限是否被要求輸入不必要的權限內容，常見如「讀取通訊錄的資料」、「讀取當下位置」、「讀取 SD 卡的內容」等，有可能為非法應用程式。

## 建議六：不使用的支付 App 請適時解除安裝

隨著電子支付愈加盛行，民眾常常會有為了點數回饋之類的促銷活動而下載支付 App，最後卻不怎麼使用的情況發生。對此，簡勝財認為，此舉有可能會有遭到不當利用以及情報洩露的風險，因此除了刪除上面用來儲值用的信用卡及銀行戶頭，也建議直接移除程式。

## 建議七：開啟螢幕鎖定功能

有載入行動支付的裝置，請務必開啟螢幕鎖定的功能，螢幕解鎖方式有帳號密碼、指紋、臉部辨識等的生物辨識系統可以選擇；若是遇到偷竊，遺失等情況，第三者也很難進行不當操作。

## 建議八：開啟 GPS跟尋找裝置功能

預防手機被偷或遺失等情況，請開啟「尋找我的 iPhone（iOS）」或「尋找我的裝置（Android OS）」運用連結網路的筆電等裝置就能查明手機的位置。

## 建議九：在家庭網路閘道端建立保護機制

民眾可以透過路由器的安全設定、變更無線網路名稱（SSID）、使用能夠保護家庭網路的資安產品等方式，防護智慧家庭網路和連網裝置免遭駭客攻擊與隱私外洩風險。

綜上所述，可見駭客攻擊手段層出不窮，且智慧型手機普及，目前可說是人手一機，加上今年新型冠狀病毒疫情影響，更讓許多人必須透過網路聯繫，或是進行遠距工作、上課，也使駭客更容易抓住使用者上網行為輪廓，藉此發動精準攻擊。總之，病毒攻擊不會只針對企業，個人也要注意，個人端的電腦病毒防護也不容忽視。