安全使用公用 Wi-Fi 的提示

不良行爲人會在網上利用您。如果您需要使用公用 Wi-Fi 時，請閱讀以下可供考慮的一些提示。

爲因應冠狀病毒疫情爆發及關閉商務和圖書館，我們許`多人花更多時間上網。結果是，我們需要使用公用 Wi-Fi 連接網際網路。如果您發現自己需要使用公用 Wi-Fi 時，請考慮以下 來自該州首席隱私官 的建議以幫助保護您的資料:

1. 確認您有正確的網路。

確定您連接上對的網路。不良行爲人以他們的名字爲基礎創建看似無害的網路，然而事實上卻指導您連接網路設定以便觀看您瀏覽網頁。這意味著，如果您在網站輸入登錄憑證或密碼，駭客將能偷走您的資訊。爲了防範這種事情發生，如果可能的話，請非常仔細地閱讀網路名稱，要求員工或檢查行業標示牌以便確定網路是合法的。

知名網路如這些熟悉的咖啡連鎖店，不太有嫌疑，因爲公司經營網路就像是他們的企業的一種服務。知名網路通常比在公共場所顯示在您的手機上的 隨機免費 Wi-Fi 網路還要安全。

2. 關閉自動連線。

許多裝置 (智慧型手機、筆記型電腦和平板電腦) 有自動連線設定。此設定讓您的裝置順利連接附近的網路。用這樣的方式連接可信任的網站是可以的，但是也會讓您的裝置連接到不安全的網路。您可以通過您的裝置上設定功能停用這個功能。保持這些設定關閉，尤其是當您前往不熟悉的地方旅行時。使用公用 Wi-Fi 後您可以檢查「忘記網路」，當作額外的防範措施。

在公共場所時，您還應該監視您的 Bluetooth（藍牙）。Bluetooth（藍牙）連線讓各式各樣的裝置彼此通訊，駭客可以找到打開的 Bluetooth（藍牙）訊號入侵您的裝置。當您在不熟悉的地區時，留著您的手機上這項功能並且將其他裝置上的這項功能關閉。

3. 關閉檔案分享。

打開公用 Wi-Fi 時，請確定關閉檔案分享選項。依您的作業系統而定，您可以從系統偏好設定或控制面板上關閉檔案分享。AirDrop 是一種您會想要關閉的檔案分享功能的範例。首次連接到一個新的公用網路時，一些作業系統如 Windows/PC 會透過選擇「公用」選項爲您關閉檔案分享。

關閉檔案分享的步驟

在 PC 上時:

1. 前往網路分享中心。
2. 然後 變更進階的分享設定。
3. 關閉檔案和列印分享。

針對 Macs:

1. 前往 系統偏好設定。
2. 選擇分享。
3. 取消選擇所有選項。
4. 接下來，在 Finder 上，點選 AirDrop，然後選擇 讓我不被任何一個人發現。

針對 iOS，只須找到控制中心內的 AirDrop，然後將它關閉。

4. 使用 VPN。

考慮在您的裝置上安裝 VPN (虛擬私人網路)。對於公用 Wi-Fi 數位隱私權而言，VPN 最安全的選項。當它穿梭您的裝置充當保護性「通道」時，它會幫您的資料加密，如此，當它通過網路時，您的資料就不會被看見。

5. 關於 FBI 對於加密網站 – HTTPS 的警告。

FBI 曾警告過 關於以"https" 開始的網站位址。"https" 的出現及鎖定圖示應該是用來表示網站流量被加密以及訪客可以安全地分享資料。然而，電腦犯罪如今透過引誘人們前往加入 https 的惡意網站並且當這些惡意網站不安全時顯示安全來指望大眾能信任。

FBI 的建議:

- 不要輕易相信電子郵件上的名字: 質疑電子郵件內容的意圖。
- 如果您收到來自已知聯絡人的含連結的可疑電子郵件，請透過致電或電子郵件傳送給該聯絡人確定訊息是合法的。請勿直接回覆可疑的電子郵件。
- 檢查連結中是否拼寫錯誤或錯誤網域 (例如：應該以 ".gov" 結尾的位址是否以 ".com" 結尾來取代)。
- 請別只因爲瀏覽器網址列中有鎖定圖示或 "https" 而信任一個網站。

6. 不建議存取敏感的資訊。

即使您有 VPN，仍然不建議 在安全的公用網路上存取個人銀行帳號或類似敏感的個人資料如社會安全號碼。甚至公開的安全網路也會有風險。如果您必須在公用 Wi-Fi 上存取這些帳號，請運用您的最佳判斷。至於金融交易，最好使用您的智慧型手機熱點功能來取代。

7. 安全的網路對照不安全的網路。

基本上，有兩種公用 Wi-Fi 網路: 安全的網路與不安全的網路。

一有可能連接到安全的公用網路。無須任何一種安全特性如密碼或登入，就會連接到不安全的網路。連接到網路前，通常，安全的網路需要使用者同意條款與條件、註冊帳號或輸入密碼。

8. 保持防火牆啓用的狀態。

如果您正在使用筆記型電腦，開啓公用 Wi-Fi 時，請保持防火線啓用的狀態。防火牆擔任保護您的手機免受惡意威脅的屏障。由於彈出通知然後忘掉它，因此使用者可停用 Windows 防火牆。如果您想在 PC 上重新啓動它，請前往控制面板，「系統安全檢測，選擇「Windows 防火牆」。如果您是 Mac 使用者，請前往「系統偏好設定」，然後前往 安全與隱私，然後到「防火牆」標籤以便啓動該功能。

9. 使用防毒軟體。

還要確定在您的筆記型電腦上安裝防毒程式最新版本。使用公用 Wi-Fi 時，防毒程式可幫助保護您，使用共享的網路時，它透過偵測可能侵入您的系統的惡意程式。如果知道有病毒被載入您的裝置上或如果有任何可疑活動，或者如果惡意程式侵入您的系統，會有警訊警告您。

10. 使用雙因素認證或多重因素認證。

當登入有您的個人資訊的網站時，請使用多重因素認證 (MFA)。這意味著，您有第二個驗證碼 (用簡訊傳到您的手機或透過 app 或實體金鑰提供)，可進一步保護您。因此即使駭客取得您的使用者名稱和密碼，沒有驗證碼，他們便無法存取您的帳號。

11. 追蹤您的裝置。

請勿 將筆記型電腦、平板電腦或智慧型手機留在公共場所或汽車內而無人看管。即使您對於 Wi-Fi 網路有防範，也無法阻止某人奪走您的財產或偷看您的資訊。請注意您的四周圍並留心那些在您身旁的人。

12. 其他網上安全提示。

這裡有一些保持安全上網的提示，尤其是您如果使用公用 Wi-Fi 連線:

- 使用強密碼。
- 將您的裝置加密。
- 提防網路釣魚電子郵件。
- 小心您張貼在社交媒體上的東西。太多個人詳細資料可以幫助駭客猜到密碼。

- 刪除您不再需要的舊資訊。
- 如果網路要求您安裝任何額外的軟體或瀏覽器擴充功能，請勿連接。
- 確保在您的裝置上安裝最新的修補軟體更新以防護已知的問題。