

Wi-Fi 走到哪連到哪？一不小心就連到地雷啦！

現代人絕對不可以缺的生命要素，就是「Wi-Fi」，每天「出門在外、尋找 Wi-Fi」也成了一種日常。

不過，Wi-Fi 可不能隨便連，否則一不小心洩漏了資料，甚至讓手機故障，可就得不償失啦！

用了 Wi-Fi，秘密全都看光光？

公共場所的 Wi-Fi 開放網域，是駭客竊取我們資料的最佳管道，一定要謹慎小心，不然很容易讓個人資料外洩。

如果真的需要使用時，一定要記得在加密的狀態下使用，比如說：連到有「https」的網站，或是透過 VPN（虛擬私人網路）來建立安全連線。

還有，有些駭客會假意提供免費熱點，讓我們在不知情的情況下使用，藉此蒐集我們的網路足跡和密碼等資料，所以，可別因為貪小便宜而隨意連接不知名的 Wi-Fi 喔！

這種 Wi-Fi 竟然會直接癱瘓手機！？

除了上面說的資安風險，2021 年還出現了一種全新的陷阱，那就是：含有「%」的 Wi-Fi！

有國外資安研究員發現：只要用 iOS 裝置連上名為「%p%s%s%s%n」的 Wi-Fi，就會強制關閉 iPhone 的 Wi-Fi 功能，如果想要重新開啟，就只能重置手機網路的設定。

為什麼會這樣呢？這主要是因為 iOS 裝置的手機系統有字串格式化漏洞（Format String Bug）的問題，當 iOS 裝置連上名稱中含有%s 或是%p 的 Wi-Fi 時，會觸發漏洞導致裝置無法正確地處理這些 Wi-Fi 名稱。當我們沒有為程式設定好防護機制時，攻擊者就可以用這些特殊字串來欺騙程式，藉此取得手機中的資訊和控制權。

記得下面這 3 點，Wi-Fi 也能輕鬆連！

沒想到 Wi-Fi 的陷阱這麼多！但我如果真的需要用到的話，又該怎麼辦呢？別擔心，只要記得下列 3 項原則，就可以避開陷阱喔！

- ✚ 關閉手機「自動加入熱點」的功能：要連 Wi-Fi 前，一定要先確認它的安全性，所以，盡量手動篩選，不要讓手機自己連，就可以避免連上惡意 Wi-Fi
- ✚ 不使用公開、安全性未知的 Wi-Fi：隨便搜到的公開 Wi-Fi 雖然方便，但卻不一定安全，應該要盡量避開。可以選擇使用縣市政府所設置 Wi-Fi，並且在使用前注意相關隱私條款，才能用得安心喔！
- ✚ 即時更新手機作業系統軟體版本：手機軟體版本要定期進行更新，讓系統為你修復安全性漏洞，才能用最好的狀態防範資安陷阱

資料來源:教育部全民資安素養網

資料日期：111-07-08

