

愈來愈多公司採用無線區域網絡（WLAN）。根據Gartner的估計，美

國已有三成的公司裝有WLAN。WLAN的好處是方便安裝費用廉宜。不過，閣下有否考慮其安全性呢？

最近專業資訊保安協會（PISA）做了一個有趣的研究，反映目前本港公司在使用WLAN時面臨資料外洩的危險亦不自覺。據PISA的主席梁兆昌表示，調查於本月7日（星期日）中午時分進行。PISA的調查員帶着裝有LAN卡的手提電腦及天線乘坐電車從金鐘到堅尼地城，然後再坐電車折返銅鑼灣。

在短短的車程上，調查員已可連接一百八十七個WLAN轉接站。當中更發現七成的WLAN轉接站沒有開啓加密系統。超過五成的WLAN轉接站仍然使用產品原設定或眾所周知的service set identifier（SSID）。調查更發現路途上有十個地點的訊息十分強勁，隨時可連

對無線網絡提高警覺

接上，這個不排除是有兩個辦公室在不同大廈採用WLAN來傳遞訊息。被非法使用者連接上，有被盜用資源、竊取敏感資料、散播病毒及破壞系統等後果。

大家可想想，調查在星期日進行已是這樣子，若在上班繁忙時段，相信情況更嚴重。由於目前WLAN的保密機制仍不夠完善，故各使用WLAN的公司須做好一切防禦措施，確保較難被外界入侵。以下是應注意的事項：

一、開啓加密系統應使用128位元加密。有些較早期WLAN的產品是用40位元加密，很容易就能被破解。

二、公司要禁止員工自行安裝WLAN，並定期巡查。

三、更改已設定的SSID，以及不要廣播SSID予外界人士。要知道愈少人得悉貴公司的設定，被入侵的機會愈小。

四、公司網絡要設有防火牆，更不應把WLAN轉接站設在公司網絡內。

五、更改已設定的用家名稱及密碼，更要使用一個較為複雜的密碼。

六、設立網路卡卡號（MAC address）登記制度，只容許授權LAN卡擁有者進入公司WLAN內。

無線科技不限於WLAN，還可在廣域無線通訊，如3G、GPRS或個人區域網絡如藍牙等。無可置疑，通訊科技不斷發展，無線科技將成爲一個重要環節。但如果用戶把無線聯想爲資料外洩的不安全傳遞方法，想必減低他們使用的興趣。所以其未來發展不只是改善素質、加快速度，還要是安全可靠。

朱文英

香港生產力促進局
軟件業資訊中心研究主任