無線網路安全

www.aoema.org

網路世界讓你覺
得不安全嗎?

使用本手冊
來保護你的
無線電腦網路

無線網路安全

介紹

在充滿無線通信的今日世界裡，隨時隨地都可能運用無線網路，例如：在家中各處使用你的筆記型電腦工作或收發電子郵件。從機場、餐廳或旅館連接你辦公室的電腦網路。從會議室或公司的自助餐廳收取檔案、瀏覽網站或傳送即時訊息給同事。

然而，方便性和靈活性是有代價的 - 安全威脅程度隨著無線網路的使用而增高。使用者必須了解這些問題並學習如何在問題發生前做出防範。本手冊將會幫助你設定無線網路，並建議你如何安全地透過公用的無線網路熱點來使用網路。

請不要將本手冊當成是你的無線裝置隨附操作手冊的替代品，請將它當成一個補充說明來幫助你設定你的硬體以達到可能的最高安全層級。

本手冊的大部分內容無關技術層級，因此適用於所有使用者。不過，在第12和13頁的資訊多是提供給進階的使用者而非初學者參考。

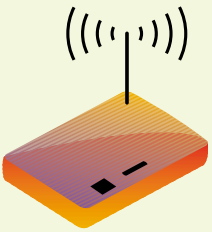
目錄

本手冊附有專有名詞的詞彙表，供需要時參考。如果你先花個幾分鐘讓自己熟悉一下無線傳輸科技的字彙，你將會更容易了解本手冊的內容。前9個專有名詞對所有的使用者都很重要，而最後4個則是供進階的使用者參考。

在讀這本手冊時你需要知道什麼?

藍芽 (Bluetooth)	藍芽是一種無線傳輸技術的名稱，主要使用於個人裝置間之短距離通訊，而非使用於電腦網路。例如運用藍芽於電腦與個人數位助理和行動電話的通信傳輸，可以讓你的電腦無線連接印表機或掃描器等週邊裝置。
媒體存取控制位址 MAC Address (Media Access Control)	任何連接到網路的裝置(例如：網路卡、無線網路卡或無線網路基地台)都需要一個唯一的識別碼，以做為媒體存取控制位址之用。MAC位址是一系列用冒號隔開的數字，例如00：07：40：A2：1A：BB。通常你可以看到這個位址印在網路裝置表面的小標籤上。另外，也可以藉由詢問指令來查詢裝置的MAC位址。
網路加密機制 (Network Encryption)	• WEP：「有線等效私密協定」是Wi-Fi(無線相容性認證)網路的基本安全功能，能將訊息以40位元和128位元的加密方式譯成密文透過無線網路傳輸。惟WEP已被證實可輕易被破解，有很多工具可以自由地截取加密訊息並在十分鐘裡破解你的WEP金鑰。故建議使用其他加密措施來取代WEP的使用；雖然如此，若無其他選擇，使用WEP總比完全沒有任何加密措施要來得好。 • WPA：「Wi-Fi保護存取機制」係由Wi-Fi組織研發，提供改良的數據資料加密措施和使用者認證機制。只有金鑰符合的電腦才能存取你的無線網路。最新的電腦作業系統版本(Windows XP, Apple OSX, Linux)都已提供WPA安全機制。
惡意無線基地 (Rogue Access Point)	網路上未經授權的無線基地台。

服務設定識別碼 (SSID)	SSID係指「服務設定識別碼」，是一個無線網路的名稱或識別碼，它可以是任何字母(可包含大小寫字母)和數字所構成的字串，最長可輸入32個字元。無線網路基地台的製造商會在出廠時預設SSID碼，但建議你更改這個設定來防止侵入者，或避免附近使用同型式之無線網路基地台的鄰居，意外地進入你的無線網路。 SSID關連到不同的專業術語，包括電腦網路名稱、優先的電腦網路、ESSID (延伸服務設定識別碼)或無線局部區域網路服務區域。任何連接到你無線網路的裝置都要知道你的SSID。
傳輸控制/網路通訊協定和網路位址 (TCP/IP and IP Addresses)	傳輸控制/網際網路通訊協定－電腦間用來溝通的語言，網際網路使用這種語言讓你可以瀏覽世界各地的網頁。 TCP/IP要求每一連接到網路的機器或裝置具有唯一的網路IP位址，通聯的數據封包必須包含有來源網路位址和目的網路位址，始可傳送。 和電話號碼類似，IP網路位址的格式是由四個0~255的數字所組成，例如123.213.154.178，讓電腦網路能識別這個裝置。有些網路位址已被指定為私有位址，無法直接由公用的網際網路連結。
無線網路存取點 (Wireless Access Point)	家庭或小型辦公室無線網路的核心，稱之為存取點（有時亦被稱為基地台），是一個提供無線裝置連接入口的設備。你可以把它想像成“交通警察”指揮你無線網路裡的數據資料，如果需要時，亦可管理無線和有線網路間傳輸封包的數量。市面上有許多無線網路基地台的製造商，包含Netgear、Buffalo、Linksys、D-Link和Cisco，價格由$US75起不等。你可以基於何種“802.11”標準最適合你的需求、或是裝置所能提供的特點和功能(包含安全功能)及預算等不同條件做為購買的考量。
無線網路模式 (Wireless Network Modes)	“802.11”標準定義有兩種網路模式： • 基礎架構模式 －無線裝置間互相溝通要先透過一個基地台，它是和有線網路間的介接，也可以獨立運作。 • 對等(Ad-Hoc)傳輸模式(也被稱為點對點或電腦對電腦)－無線裝置間可直接傳輸，而不需經過基地台。 使用無線網路對等傳輸模式時無須購買額外的硬體即能提供快速和簡易的無線網路，但會有衍生的安全問題，因此最後決定採用何種模式前，必須先確認額外的安全問題。
無線網路 (Wireless Networks)	• Wi-Fi(Wireless Fidelity) :無線網路可讓多台電腦和裝置在沒有實體連接的情形下做通訊，因此不需要用到纜線。現在絕大部分的無線網路都被稱為Wi-Fi。

	• 標準：美國電子電機工程師學會(IEEE) 發展出一系列標準來界定裝置如何透過無線電波來通信，且賦予它一個系列編號“802.11”。“802.11”系列有好幾種標準，下面列舉出可供選擇的種類。你可依價格、性能和相容性來決定那一種比較適合。 o 802.11g－快速的數據傳輸率，相對而言價格較低，受電波干擾的風險較高。 o 802.11b－非常近似且相容802.11g的裝置，但以較低的速率做數據傳輸。 o 802.11a－因它並未和802.11b/g一樣分享行動電話和微波爐的頻率(2.4 GHz)，具低電波干擾風險，並有更多的頻道供802.11a 的裝置來更進一步降低電波干擾的問題。 o 802.11n－根據之前的802.11標準建立，增加了多重輸入和多重輸出的功能。額外的傳輸和接收天線能容許較大的數據資料傳輸量。 o 802.11i－一種新的安全標準，WPA標籤可以用來證明符合802.11i協定子集的裝置。WPA2標籤證明該裝置完全支援802.11i標準。你所使用的基地台，不論是802.11a、b、g或n都應包含WPA或更好的WPA2功能。 想瞭解“802.11”系列的完整清單，請參考Wi-Fi聯盟的網站www.wi-fi.org。Wi-Fi聯盟為一非營利的企業組織，負責測試和認證所有使用“802.11”標準的裝置。
動態主機組態協定 (DHCP)	動態主機組態協定負責分配IP位址給任何提出要求的裝置。部分無線網路基地台已預先安裝了DHCP，能自動分派IP位址給連接到電腦網路的所有裝置。此方便性對需要使用不同網路的筆記型電腦使用者來說特別好用，但同時也有安全風險。如果有人允許被進入網路，DHCP會自動提供一個有效的IP位址。所以，如果你不能限制DHCP分配位址，最好關閉這個功能。
撥號用戶遠端認證服務協定 (RADIUS)	撥號用戶遠端認證服務協定(RADIUS)是一種對使用者從遠端連接到他們辦公室電腦的認證方法。此協定同樣可以應用在無線網路使用者的認證。
遠端加密安全登入 (SSH)	SSH代表一種安全通道，是一個比遠端終端機存取(Telnet)更具安全性的工具。Telnet是一種執行遠程登入的工具，以便連上遠端主機。 SSH用來獲取可存取遠端電腦的安全命令執行列，也可透過安全的”通道”來傳送其他類型的數據資料(如：檔案傳輸協定等)。
虛擬私有網路 (VPN)	虛擬私有網路，兩台電腦間透過網際網路做端點對端點的安全連結的方法，也可用在無線網路的安全通訊上。

爲你的問題找尋答案：

當設定一個無線電腦網路時，你可能會問的問題：	參考頁面：
我該選擇“電腦對電腦”或“基礎架構模式”？	“電腦對電腦”是最簡單又便宜的模式，但“基礎架構模式”則比較安全。你應該了解兩個模式間的差異處，以做出正確的決定。 第8頁
我該把無線網路基地台(AP)設置在哪裡?	無線網路基地台(AP)的實體位置可能會影響性能和安全，請參考10項簡單的建議，使兩者皆能有最大功效。 第9頁
我該接受無線網路基地台上的原廠設定或改變它?	當你取出無線網路基地台後，它的部分功能會有原廠設定值。你必須決定接受這些設定值或更改它們。你可參考建議配置設定的圖表，以了解如何安全的設定你的無線網路基地台及保護你的無線網路。 第10頁
我該如何保護我的無線網路?	設定無線網路時，第一步為安裝無線網路基地台。你必須了解10項附加的建議，並確認它們是否適合。 第12頁
我要如何在現有的有線網路上加入無線網路?	當結合無線網路至有線網路時，你必須確認無線科技特定的安全考量以保護整個網路。 第12頁

參考頁面：	當使用無線網路科技時，你可能會問的問題：
提供6項簡單的建議來保護你的筆記型電腦和儲存的數據資料。每次使用時，每一步都要依照這些簡單的步驟。了解它們，你就可完全利用公用的無線網路熱點。 第14頁	透過公用的無線網路熱點，使用我的筆記型電腦來收取電子郵件和瀏覽網站，是否不安全嗎?
這6項簡單的建議裡有部分需要更改你的筆記型電腦設定。它們很容易被設定且幾乎不用花多少時間。不過，重要的是當你每次想使用公用的無線網路時，要檢查這些設定。 第14頁	我需要更改我的筆記型電腦設定嗎?

現在很多行動電話和個人數位助理都有網際網路的功能，使得它們也和筆記型電腦一樣有安全風險。譬如說，你知道所有的行動裝置上都該安裝防毒軟體(Anti-Virus)和防火牆(Firewall)嗎？ 第16頁	透過公用的無線網路以我的行動電話或數位個人助理(PDA)來使用網際網路會如何?
由於藍芽裝置是透過開放的無線電波傳輸，會有潛在的風險，所以要了解這些風險及學習使用防範措施。 第18頁	藍芽科技安全嗎?
違法、有意圖的行動，可能違反相關的法律條文。令人擔心的是，守法的個人因沒意識到無線科技已受法律保護，而犯下無預謀的違法行動。 第20頁	使用無線連接有任何法律上的考量嗎?
有線、無線的網路或獨立的電腦，都有一些連接網際網路時該依據的實施標準。 第22頁	一般來說，我該如何保護我的電腦和數據資料?

Wi-Fi裝置有兩個模式可以使用：

- 基礎架構模式 – 使用無線網路基地台(APs)當成無線裝置連接的存取點。
- 點對點或電腦對電腦傳輸模式 – 在此模式下，無線裝置直接連接到其他的無線裝置，不需使用無線網路基地台。

點對點傳輸模式經常於“無線網路點對點傳輸模式”(或單次傳輸)的情形下，被使用在兩台或更多電腦間的數據資料交換。有些使用者選擇點對點傳輸模式，是因它是設定無線網路簡單又便宜的方法，並可省下無線網路基地台的費用。

20字的密碼。這樣任何試圖連接你電腦的人必須精確地知道你設定的密碼。

最好的建議是任何時候都不要使用點對點傳輸網路模式，如果必須使用，請在不用時關閉它。這可以在Windows XP作業系統“無線網路”設定畫面裡的“進階”選項畫面裡完成設定，並永遠不勾選“自動連線到非慣用的網路”。

8

選擇你的無線網路模式

然而，當使用點對點傳輸模式時，有些由無線網路基地台所提供的保護措施便無法取得。絕大多數的大型公司禁止所有的網路使用點對點傳輸模式，因為他們認為這對他們的電腦網路及所儲存的數據資料有安全上的風險。因點對點傳輸網路沒有使用工具來驗證使用者，範圍內的”外部”裝置可以連接允許點對點傳輸的任何”內部”裝置。雖然每個裝置必須在同一個頻道上，使用同一個SSID和IP子網路，但對有經驗的“怪客(Cracker)”來說，他們可以解決這瑣碎的問題。

如果你有理由允許點對點傳輸網路，請確定你有使用WPA加密，且含至少15至

建議

- 當不使用時，永遠關閉點對點傳輸網路。
- 當使用點對點傳輸網路時，永遠使用WPA加密。
- 如果沒有WPA加密，使用WEP加密。
- 使用堅固的密碼 (建議使用15至20字元的密碼)。
- 使用適當的無線網路基地台來替代點對點傳輸網路。

首要考量是無線網路基地台的實體放置位置。基地台的位置牽涉到性能的問題，也同時關係到安全的問題。

建議

- 將基地台安置在你的無線網路服務區域中心點。
- 儘可能安置在所有電腦的視線範圍內。
- 減少無線網路基地台和電腦間的牆壁或天花板數目。
- 設置無線網路基地台在合適的位置上，例如：高的書櫃上，以提高接收的敏感度。
- 讓無線網路基地台遠離金屬表面，包括實心金屬門、金屬的書桌及文件櫃。水也可能降低性能，例如：魚缸或大型盆栽。

配置你的無線網路基地臺

無線網路基地台是用無線電波傳送和接收。為了保護在網路裡傳送的數據資料，你應儘量降低無線電波洩漏至指定的服務區域以外。

除了電波外漏的考量外，你也要保護你的無線網路基地台不被未經授權的人竄改，他們可以按下重設鍵讓所有的設定回復到原廠設定，讓你保護這個裝置的心血通通白費。這也可以避免配置”舊”設定的電腦使用無線網路基地台。

- 避免電波干擾，遠離微波爐和2.4GHz的無線電話。
- 為減少電波外漏至指定服務區域之外，儘可能降低廣播的輸出功率。
- 遠離外牆／窗戶和普通牆壁與住家／辦公室毗連，以確保信號不會延伸至需求的區域外。
- 試著將它安置在安全的地點，以確保未經授權的人不會竄改你的無線網路基地台。
- 有些無線網路基地台允許你降低輸出功率，以防止因信號太強，導致電波外漏至指定服務區域外（經過門口或窗戶），使得“外面”的區域得以使用。

設定你的無線網路基地臺

功能	原廠設定	安全的設定
使用者名稱和密碼	設定依製造商而有所不同，但兩個最普遍的使用者名稱為“admin”和“root”，最普遍的預設密碼包括“admin”、“password”和沒有任何字元的空白。	**更改使用者名稱和密碼** 所有的無線網路基地台允許並鼓勵你更改預設的密碼。然而，有些基地台不允許變更使用者名稱。
廣播網路名稱(SSID)	開啟	**關閉** 不要允許無線網路基地台的名稱或SSID被廣播。如果廣播SSID的功能無法被關掉，“信標間隔”(Beacon Interval)就該被增加至最大值。
無線網路名稱或SSID	有些出廠設定的例子，包含： NETGEAR DWL-2100AP AP+(MAC 位址)	**更改名稱或SSID** 很多無線網路基地台有預設標準名稱或SSID，這些名稱很容易地從製造商的網站上得到。
加密(WEP/WPA)	關閉	**開啟** 有兩種加密方式：WEP (有線等效私密協定)和WPA (無線保護存取)。WEP是舊的方法，被認為不能勝任現在的標準。現在所有的無線網路基地台幾乎都提供並建議設定含128位元加密的WPA。
驗證型式	自動	**開啟驗證功能**
MAC位址過濾	關閉	**開啟** MAC位址是分配給每台電腦網路卡的獨特識別碼。很多無線網路基地台有能力去自動建立被允許使用無線網路之MAC位址清單。
DHCP	開啟 對於可以互相通訊的電腦網路，每台都必須在相同的“子網路”上有IP位址-這就在同一個郵遞區號裡的不同住址或同一個區域碼裡的不同電話號碼一樣。	**關閉** 有些無線網路基地台提供DHCP的功能，但有些沒有。如果有的話，你應該關閉它。

爲什麼這是重要的	注意!
大部分的無線網路基地台有相同的預設使用者名稱和密碼(原廠設定)，表示任何人都可以進入你的網路來更改你的基地台設定。	如果你忘記了密碼，你必須重新設定基地台才能得到進入的權利，這表示你必須再次設置無線網路基地台。
無線網路基地台的名稱或SSID。廣播你的SSID等於告訴每個人你的無線網路存在，且每個有相容裝置的人可能和你的無線網路建立連結。	希望連結你無線網路的任何人必須手動輸入SSID以得到使用的權利。你電腦上的軟體將無法自動找到無線網路基地台。
如果你保持原廠設定，即使你關閉廣播SSID的功能，有人還是可以猜測它。你必須更改SSID來避免這種情形。	新的SSID名稱不該和你的任何事物有關，如：你的公司、住家環境或地理位置。

有兩種方法可以更改無線網路基地台設定：一是從無線網路，二是以USB或實體纜線連接至無線網路基地台，其中實體連接會提供附加的安全功能，所以是更改安全設定的最好方式。在無線網路基地台上，應該確實地關閉從無線網路做更改設定的方式。

你可以保護你的基地台和無線網路，但因網路是用無線電波傳遞，不懷好意的人還是可以截取無線網路傳輸的數據資料，這就是為什麼開啟加密功能和使用更強的WPA標準，是如此重要。	所有連接到無線網路的裝置必須使用WPA加密功能。在同台無線網路基地台上不可能混用WEP和WPA的功能。 當使用WPA加密時，建議設定20個或更多字元的密碼，這密碼會很難記住，但有些套裝軟體能安全地記憶你的密碼。
共享金鑰(Shared Key)的機制應不再被使用。它可能讓金鑰在幾秒鐘內被洩露，公開認證功能(無效/無認證)永遠比共享金鑰來得好。	已不再建議使用WEP加密，但你的裝置在未配置WPA或WPA2加密的情形下，你還是必須使用它。
手動建立MAC位址清單將限定已知的裝置能使用你的網路。使用MAC位址過濾，你可以有效的將基地台被濫用的機會降到最低。	必須包括你自己電腦的MAC位址，否則你將沒有使用權。 MAC位址並沒有加密，使得不懷好意的人可能在你的網路上偷窺MAC位址來符合你設定的位址，進以得到使用網路的權利 。 不過你可根據本手冊裡的建議，將這種情形的發生機率降到最低。
DHCP會自動分派獨特的網路位址給網路中的每台電腦，它讓我們可以簡單地新增電腦或其他裝置至無線網路中。 然而，這個自動的功能也使未經授權的人更輕易地進入你的電腦網路，所以最好關閉這個功能。	關閉這個功能後，你必須手動輸入網路上電腦和個人數位助理的IP位址。雖然有點不方便，但全面地增加無線網路的安全性。

除了無線網路基地台的必要設定外，還有其他設定可以用來保護你的整個網路環境。下面列出建議事項，幫助你更進一步增加安全性。

12

保護你的電腦網路

建議	爲什麼這是重要的
用軟體偵測網路上的窺視者	現在有些軟體允許你看見所有連接到你網路的裝置，另有些流行的防毒軟體亦包含此工具。當不明電腦連接到你的網路時，使用這個軟體能讓你察覺它們。非經授權而安裝在你網路裡的“惡意無線基地台”也能用同樣的方法偵測出來，或經由無線網路基地台偵測軟體偵測到不明之無線網路基地台。這些”惡意無線基地台”可能是家人或同事在無惡意下安裝的，他們不知道可能會造成安全性風險，這也說明了藉由教育訓練來提高資安認知，永遠是保護網路的首要工作。
在不使用時關閉所有的無線網路基地台(例如: 在辦公室內數小時不用或週末時)	夜晚或週末期間不使用無線網路基地台時，你該關掉它。
在企業裡訂定並管理無線網路使用的安全政策	在辦公室的環境裡，要確定員工了解使用無線裝置和網路有安全上的問題，否則他們不會察覺到威脅性。寫一份具廣泛性的無線安全政策文件將增強企業的內部安全。這個政策必須結合企業所有的通訊和電腦網路政策。除非大家會閱讀和了解這個政策，不然就不值得寫在紙上了。企業一定要教育員工關於政策所列出的問題。
如果可能，更改預設的子網路位址範圍	保護無線網路的竅門就是儘可能設置障礙來妨止未經授權的人使用。選用不同的網路位址範圍來取代標準值，會使未經授權的人更難猜測出正確且可使用的網路位址。 ***警告：*** 如果使用微軟的“網際網路連結分享”功能，則不能更改使用的位址範圍。

建議	爲什麼這是重要的
開啟記錄並經常查閱紀錄檔	多數無線網路基地台有記錄無線網路上活動的功能，保存這些紀錄並經常分析它們，以發現未經授權活動，是良好的習慣。 ***警告：*** 你也許需要額外的軟體來收集、維持和分析這些數據。
用網路上常見的多種工具來測試你的無線網路安全性	除非你測試你的設定，否則永遠無法確定它是正確運作。你可在家裡或辦公室中花幾分鐘進行基本測試，無須傷太多腦筋。 ***警告：*** 有時測試會造成你自己網路的傷害，所以請事前考慮並小心測試。
用額外的認證伺服器驗證登錄的無線網路使用者	雖然你用各種加密協定來保護你網路的所有數據資料，但用一個RADIUS(撥號用戶遠端認證服務協定)伺服器來驗證網路上所有的使用者仍屬良好習慣。除非你或你的技術人員有足夠的經驗來設定這種協定，不然你會降低你網路的安全性。要知道設置一個有效的RADIUS伺服器環境是件不容易的事。 ***警告：***你必須確認所購買的硬體支援RADIUS伺服器。
當在有線網路上增加一個無線網路時，應確認兩者之間有防火牆	多數有線網路對網際網路有安裝防火牆的界面，以確保他人無法從網際網路進入私人有線網路。如果雇員想從家裡撥號進入公司網路，他們將會穿過防火牆，由於無線網路不安全的本質，因此把雇員使用無線網路看成和從家裡撥入一樣，最安全的方法是用防火牆來隔開有線及無線兩個網路。 ***警告：*** 在小型或家庭式的辦公室環境裡，安裝防火牆會增加成本，如果使用WPA/WPA2加密的話，可能就不需要。
用虛擬私有網路來加密你的無線傳輸	當使用WEP/WPA加密來保護無線通信時(這是個好習慣)，可以在無線網路介接的設備上使用VPN，使想竊取網路通信的人在執行上更加困難。 ***警告：*** 由於這些新增的安全機制，在WEP/WPA加密上使用VPN將大幅地降低網路的效能。用VPN也會使在基地台間漫遊和保存數據作業更加困難。如果你使用WPA/WPA2加密的話，也許不需要VPN。
在應用程式上使用加密協定	在網路上執行的應用程式也可用加密協定來使其變得安全，這點應該是有線和無線網路的標準慣例。使用加密協定，有助於保持無線網路上執行應用程式數據之安全。

現今可供使用的公用無線網路熱點數量正在快速的增加。有部分熱點是免費，其餘是商業經營。無線網路服務提供商體認到提供安全存取的需求，而在網站上提供軟體來加強他們無線網路熱點的安全性。

免費和私人的熱點通常不提供任何安全性。在任何情形下，你需要確定你的電腦沒有可攻擊的弱點，且你的數據資料並未暴露。參照這裡提出的建議，將幫助你確認當使用公用的無線網路熱點時，你是否被保護著。

14

使用公用的無線網路熱點

建議	爲什麼這是重要的
使用公用熱點前，關閉無線網路卡的“檔案和印表機分享”協定	當你在辦公室或家裡使用網路工作時，開啟“檔案和印表機分享”協定，將會改善工作效率。它允許你分享檔案或使用連接在網路裡其他印表機，可是在使用公用的熱點時，這個協定變成一個主要的安全風險。你當然不希望一般大眾分享你的電腦檔案，所以當你在餐廳、旅館、機場和開放的無線區域等公共場所工作時，關掉這個功能是非常重要的。 ***警告：*** 當你使用自己的電腦網路時，必須記得將這個功能打開，否則，你將不能使用網路印表機列印或分享檔案。
(Windows XP 使用者)：使用公用熱點前，你應該清除“我的最愛”網路清單	Windows XP 會主動地探測和廣播你所使用的所有SSID(廣播網路名稱)。如果某個人識別出你偏好的網路，一個惡意無線基地台就可以被設定成如同你自己的無線基地台一樣。 ***警告：*** 在返回住家或辦公室的環境後，你需要重新連結你的筆記型電腦和網路。這是個簡單的步驟，只要記得刪除網路的加密金鑰、SSIDs和認證設定。
(Windows XP使用者)：在“無線網路連線”頁面下選擇只給“存取點(基礎架構)的網路”	如果你曾在“點對點傳輸”和“基礎架構”模式間切換，當要使用公用的熱點之前應檢查“無線網路連線”設定頁面，是非常重要的，因為如果你不關閉“點對點傳輸網路”的選項，其他在鄰近範圍的使用者可以在你不知情的情形下進入你的電腦，因而會有安全上顧慮。這個重要的設定很容易被忽略，並可能引起嚴重的安全性問題。

建議	爲什麼這是重要的
當使用公用的無線網路時， **(1)使用熱點供應商所提供的軟體(可從他們的網站下載) 和** **(2)檢閱網站的憑證授權證明** **(Certificate for Authenticity)**	(1) 多數公用的熱點是合法的，但有詐騙意圖的人可能設立一個假的熱點，讓它看起來像是知名的熱點(例如：T-Mobile, Boingo, Wayport)。防範此類型騙局的方法是只從供應商網站下載軟體，且只用這個軟體使用熱點。 在安裝他們的軟體前一定要先掃毒。 (2) 另一種防範惡意侵入無線網路基地台的方法是檢閱網站的憑證授權證明。簡單地按下網站畫面的鎖或鑰匙圖像，檢查並確認其憑證(Certificate) 是由真正的服務供應商(例如：T-Mobile, Boingo, Wayport)開立的，有合法的驗證服務機構(例如： VeriSign, Thawte)，且其憑證是未過期的。 透過公用的熱點來傳遞個人資訊如:信用卡細節、銀行帳號及使用者名稱和密碼等並不是一個好主意。你無法避免在開始使用無線連結時，需要和熱點服務供應商建立帳號。你可以依據上述建議1和2的防範措施，降低將自己暴露在高風險的環境中。另外，你也許可考慮申請一個低單筆交易額度的信用卡帳戶(如少於$100)，儘量只使用這個帳號來處理這種類型的線上交易。
確定所有透過公用的熱點傳送的數據資料都是加密的	多數公用的熱點沒有使用加密技術來保護網路傳送的數據資料，而是由使用者加密傳送之檔案。記住，用適當的軟體工具，無線傳輸的數據是可以被閱讀的。 基本上，你可以部署VPH、SSH或SSH通道，安全地連接你的“家用”網路。請詢問你的硬體製造商和/或網際網路服務供應商(ISP)關於更多使用和設定這些工具的細節。也有公用的服務提供VPN給個人或小型企業。 另外，基於安全性的考量可以使用安全數據傳輸的線上信箱，這個服務是由電子郵件服務供應商所提供，對任何帶著筆記型電腦且定期收取電子郵件的旅行者來說是絕佳的選擇
在使用無線網路熱點時，避免傳送個人資訊	如果你不能確定透過無線網路熱點傳送的數據資料是加密資料，最好假定它是可以被任何無線監看軟體所讀取。所以，透過不安全的網站或電子郵件訊息來傳送個人的或敏感的資訊是相當危險的。

16

使用行動電話和個人數位助理

現在有些行動電話和個人數位助理提供網際網路連線的功能，使其能在任何位置、任何時間收取電子郵件和瀏覽網頁。這些高攜帶性的裝置在機能條件上已趨近電腦，但少有使用者意識到這些先進產品的安全問題。多數人已能接受防火牆及防毒軟體，是保護資訊財產安全之最低需求。使用網際網路的行動裝置如同電腦系統一樣，容易受到病毒、特洛伊木馬(Trojan horse)、蠕蟲(Worms)、間諜軟體(Spyware)和其他未經授權的存取所影響。

建議	爲什麼這是重要的
定期備份你的行動裝置	當你的行動裝置和電腦做同步傳輸時，很多資料會存在電腦的硬碟裡。但是你通常不會備份應用程式和其他大型資料檔案。建議做週期性的完全備份以確定必要時可回復你的行動裝置。 ***警告：*** 要確認備份檔案會被儲存在可靠的媒體和安全的位置。

建議	爲什麼這是重要的
安裝防火牆	防火牆能加強連結網際網路裝置的安全防護。 ***警告*** *：* 這是個新興領域，提供給行動電話和個人數位助理使用的安全性防護軟體，對一般使用者來說，已漸漸隨手可得。你的選擇也許有限，但你應該採取一些行動，不讓你的資訊財產暴露在風險中。你可先安裝最符合目前需求的產品，持續觀察未來趨勢與發展，等待全方位的軟體程式問世。
安裝防毒軟體	所有連接網際網路的裝置都需要防毒軟體，當發送、接收電子郵件和使用簡訊服務時尤其重要。執行檔案同步傳輸時，你的行動裝置更進一步影響到你的桌上型電腦和筆記型電腦。 ***警告*** *：* 這是個新興領域，提供給行動電話和個人數位助理使用的安全性防護軟體，對一般使用者來說，已漸漸隨手可得。你的選擇也許有限，但你應該採取一些行動，不讓你的資訊財產暴露在風險中。你可先安裝最符合目前需求的產品，持續觀察未來趨勢與發展，等待全方位的軟體程式問世。
使用行動裝置的密碼保護功能	如同名稱所示，“個人裝置”經常包含個人或具敏感性資料，你不希望別人有使用它的權利。無論是找到你遺失裝置的老實人或從你這兒把裝置偷走的賊，你不會希望這些從約會到帳戶號碼等個人資訊被別人看到。開啟密碼保護功能是很容易的事，不但保護你的行動裝置，更保護和行動裝置相連結的網路裡的資料。請參考第22頁裡如何建立密碼的提示。 ***警告*** *：* 如果你忘記密碼，你的資料將不能再使用。若想繼續使用你的裝置，必須重設你的裝置，檔案儲存區的資料將被全部清除。
你也許需要安裝加密軟體	如果你在行動裝置上儲存了敏感的個人數據或公司資料時，它必須和電腦檔案一樣進行加密。 ***警告*** *：* 如果你忘記密碼，就不具使用檔案的權限。

配備藍芽的裝置使用無線電波做通訊傳輸，很多特色和Wi-Fi類似。Wi-Fi讓群組內的電腦、行動裝置和週邊設備等，不透過纜線的連接進行通訊，而藍芽則主要運用在短距離內互相通訊，不需藉由纜線傳輸。藍芽操作時使用較低的電源功率且涵蓋的範圍較小，使得別人想攔截你的信號更加困難，除非他們在你30呎範圍內。不過你必須注意關於藍芽使用上的弱點，下面要點說明幾種已知的主要攻擊類型。

這些攻擊名稱或許會讓你發笑，但事實上卻並不好笑，應該嚴肅的面對。請注意，並非所有裝置都會受到本文提及各類攻擊的影響。你應該參考製造商的操作手冊和網站，以獲取更多資訊和可能的警告。為了預防起見，最好在不使用時，永遠關閉藍芽功能。

使用藍芽裝置

偷取攻擊(SNARF attack)

指一個不道德的人得到進入你手機的權利並更改你的設定。最有可能發生情形是當你緊鄰他人時，譬如參加會議、餐廳吃飯、搭乘公共運輸工具旅行等等。

後門攻擊(BACKDOOR attack)

藍芽裝置透過“配對”(pairing)的機制互相通訊。部分電話有功能上的瑕疵，允許它們和之前授權過的裝置做配對，即使此裝置已從授權清單上移除。這個裝置可連結你的手機，且有使用你手機所有功能的權限。

這怎麼會發生? 有人借你的手機和他自己的裝置(如：頭戴式耳機)做配對，然後將手機

上的配對刪除。並非所有的手機都有這個弱點，很多手機已更新韌體或軟體以克服這個問題。

藍蟲攻擊(BLUEBUG attack)

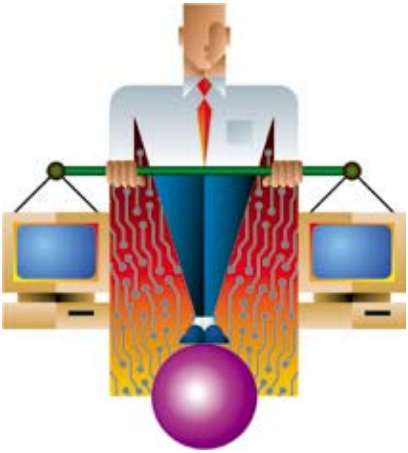
這個攻擊允許他人連結你手機裡的基本“命令集”，可以轉接你的電話，監聽你的對話和其他你不會想要的監視形式。

藍劫(Bluejacking)

藍劫大部分是無害的，鄰近的人發送惱人的簡訊至你的手機，就如同垃圾郵件一樣，令人擔心的是，它可能快速地從輕微的騷擾行為演變成危險事件。舉例來說，寄來的文字訊息要求你輸入4個數字，如果你照做，可能將你的手機和犯罪者的裝置配對，進而給予他們完全使用你手機的權利，包括聯結至儲存的資料，因此永遠不要回覆這種型式的訊息。

建議	爲什麼這是重要的
選擇不會受上述攻擊形式影響的藍芽手機和裝置	只要證實是藍芽技術上的問題，裝置製造商通常都會負責在後來的產品上解決這些問題。另外，他們常常會發布“修補程式”(patch)來解決現有裝置上的問題。沒有技術能力的人也許會覺得將修補程式安裝在他們的手機上是困難的，再買一隻不會受攻擊影響的手機容易多了。
將你的手機保持在“隱藏”模式	將你的手機保持在隱藏模式，確保未授權的人不會碰巧發現藍芽裝置的存在，而試著連結裝置。
當不使用藍芽模式時，關閉此功能	雖然視使用與否，不停地開啟和關閉藍芽功能是很不方便，但卻是保護弱點最好的方法。在不使用或不需要時關閉藍芽功能，是適用於所有環境的安全建議。

了解法律問題



當APEC(亞太經濟合作會議)經濟體和國家對於電腦相關犯罪的定義和處理方式有顯著地不同時，所有無線網路的使用者必須對現今透過無線網路進行的犯罪型態與如何保護個人和公司的財產有所認知。

惡意無線基地台 (ROGUE ACCESS POINTS)

這是依附在網路上、未經授權的無線網路基地台，通常不會通知網路管理員，即使你使用了所有我們建議的安全性措施與建議，惡意無線基地台的連結還是一個值得注意的威脅。或許是使用者的無心舉動，如買了個無線網路基地台，在不了解安全性關連的情形下，於辦公室裡安裝這個基地台，或是某人意圖用你的網路做出傷害或犯罪行為，這都可能導致公司有明顯的法律問題。基於這個理由，持續監視惡意無線基地台是很重要的。

無論如何，我們仍要提出警告，監視惡意基地台時必須要謹慎，你可能因而被控告。防範這種非故意行為最好的方法就是記得這句忠告：不要連結任何不屬於你的裝置。

偷取頻寬 (STEALING BANDWIDTH)

隨著商業和家庭無線網路使用者的增加，在無意間發現開放且能讓你上網的無線網路變得更容易。

未經網路帳戶持有人的同意而使用一個開放的無線網路，在多數的司法管轄範圍中會被認為是偷竊行為。即使並未實際違反已知法律條文之管轄範圍，偷取頻寬也必定是不光榮和不道德的行為。很多網路帳戶有下載量的限額，如果超過每個月的限額，就會有嚴厲的罰款。未經許可就用別人的網路連結視同偷竊他人。

監看 (EAVESDROPPING)

在工具容易取得的今日，透過無線網路瀏覽資料流是可

能的。透過無線網路，觀看不屬於你或你所屬組織的資料，就等同於私下盜錄通話中的對話，在多數司法管轄範圍下會被認為是犯法的行為。請注意，如果因你未採取適當的措施而使得某個未授權的人使用你的網路，而你也在尋找他們的資料時，你可能會因監看他們的行為被控告。

偷取資料

當你在家裡或辦公室工作時，你將會開啟筆記型電腦上「印表機與檔案共享」選項使得檔案交換更容易，且達到資源共享的目的，如：印表機、掃描器或網路連結。不過，如果你從公用的熱點（網路咖啡廳、機場大廳、旅管房間等等）使用有線或無線網路，你必須確定關閉「印表機與檔案共享」選項。如果你不做這個改變，你的電腦資料可能暴露給其他使用同一個熱點的人，而不誠實的人可以輕易地偷取任何感興趣的東西，這雖是不合法的行為，但也提醒你預防工作的重要性，藉以保護個人或公司的資產。

故意破壞電腦的行為

毀壞或更改不屬於你電腦上的資料是一種故意破壞的行為，在多數司法管轄範圍裡，這是會被告發的。對家庭和辦公室使用者來說，了解保護自己的無線網路以防止入侵，是很重要的。

電腦犯罪法實施後，未經授權使用電腦來毀壞、修改或改變資料，已成為不合法的行為。(解釋因使用他人電腦而違反法律)

不適當的安全性 – 企業的後果

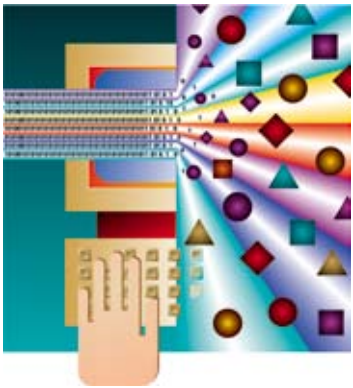
這不僅是個無線相關的問題，今日企業的負責人和經理人有重大的責任去保護和延續他們的生意。如果一筆生意因缺乏合適的安全措施而損失巨額金錢，負責人和經理人可能會發現他們處於被政府相關單位起訴的風險中。APEC隱私原則指出個人委託資訊給被授權的他人，預期他們的資訊將被以合理的安全預防措施保護。

人為干擾信號(JAMMING SIGNALS)

人為干擾，也被稱作“電波干擾”(Interference)，涉及從鄰近地區以發射器廣播信號至無線網路的裝置，試圖使無線網路超載而導致失效。在許多司法管轄範圍中，人為干擾是犯法的，唯一真正有效防禦人為干擾的方法是保護無線廣播區域免於未授權個人的侵害。

使用未被認可的無線裝備

在APEC經濟體及全世界多數的國家中，是由政府單位核定無線設備種類。請確認使用或計劃使用的設備已被政府單位批准。你也許聽過”有創意地”的使用非標準的設備以增強無線網路性能的方法，但是你可能不知道如果使用任何未被政府批准的設備，有可能會觸犯法律。舉例來說，如果裝置的信號太強，你會不小心地干擾或阻礙其他信號，如此便違法。另一個問題是使用黑市設備：它也許相當便宜，但可能不適合你的區域使用。



不管有線或無線、網路或單機，當連結到網際網路時，應遵從標準常規。以下的安全性建議將對防衛電腦和保護儲存資料有所幫助：

電腦安全性要點

將作業系統更新至最新版本

基於安全性的理由，更新作業系統至最新版本是極其重要的。所有Windows、Apple MAC和Linux的使用者應該定期至相關網站查詢軟體更新的情形。使用最新版本的好處是，得到已知安全性問題的“修補程式”，同時保護電腦和資料，免於成為別人入侵的目標。

對Windows 95和98的使用者來說，由於微軟已經不再支援作業系統，使用者為避免被攻擊，應立即將Windows作業系統更新至最新(且微軟支援)版本，或是改用Linux作業系統。除了更新作業系統之外，建議依照本節所敘述的各項方式，努力養成安全操作電腦的習慣。不管你使用的是那個作業系統，如果不遵照下列建議，還是會有安全性的風險：

警告： 在更新最新的作業系統版本前，請確認(a)你的電腦有足夠的能力去執行新的作業系統，且(b)你的應用程式和新的平台是相容的。

建立堅固的密碼

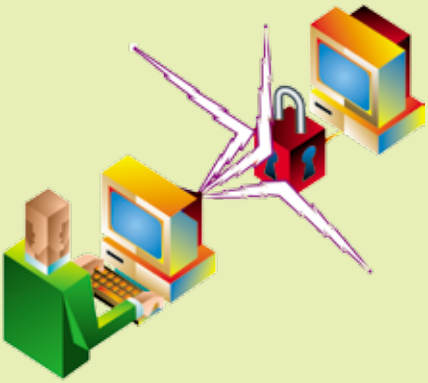
建立密碼時，應遵循經驗法則所累積之最佳建議，因駭客能在幾分鐘內破解簡單的密碼。不過，遵循這些密碼設定”注意事項”產生堅固之密碼，駭客需多花點時間才能“破解”。

- 不要用任何字典(任何語言)上可找到的字(包含術語)。

- 不要用任何字典(任何語言)中能找到的字來倒寫。
- 不要用任何和你相關的數字或文字，例如： 地址、電話號碼、生日、寵物的名字、綽號、最喜愛的體育活動或嗜好。
- 不要用連續的字母或數字，如“abcdefg”或“234567”。
- 不要用鍵盤上鄰接的按鍵，如：“qwerty”。
- 不要讓它簡單到你不用寫下來就可以記得。
- 要使用包含字母、數字和特殊字元的隨機組合。
- 要使用大小寫且含特殊字元(* @ #)。
- 要至少使用6個字元，愈長愈好。
- 無論基於任何理由，都不要把密碼給別人。
- 不要選擇某些網站上提供“記住我的密碼”的功能，把你網路瀏覽軟體裡的這個功能關閉。
- 不要使用相同密碼-有一個專門給無關緊要的操作使用，而另一個給較敏感或緊要的操作使用。
- 為了額外的安全性，每個月要更改密碼。

一個好的密碼例子就像 V-pfC~6M

警告：不要把密碼寫下來，這是使用者常犯的大錯誤，有軟體可以安全地管理你的密碼，你只要記住一個密碼就好了。所有的密碼應定期更改，大約每六星期更改一次。



在你的電腦上安裝“個人防火牆”。

安裝“個人防火牆”(Personal firewall)軟體，能保護你的電腦免於駭客侵襲，且能預防不需要的程式進入系統。也許你認為你的電腦上沒什麼值得觀看或偷取的東西，所以無需安裝個人防火牆。可是駭客有太多的理由想侵入你的電腦。

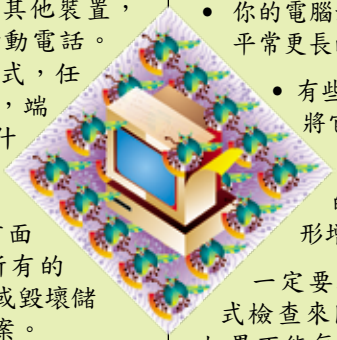
所有使用網際網路的電腦都應安裝防火牆。這不應該是可選擇的或是根據你使用網際網路的程度而定。就駭客隨機搜尋的行為而論，不定時上線和終日上線都容易受傷害。幾個主要系統供應商都有提供免費的防火牆，你可上供應商網站參考更多資訊，並下載最符合需求的防火牆軟體。你可能必須為未授權的使用者透過你不安全的網路攻擊他人而擔負法律責任，所以，必要的保護一定要做。

警告：有時從你的防火牆彈出的視窗會顯示警告，而你必須回答它的問題。確實花點時間去了解問題的本質，才能適當的回答。

安裝防毒軟體

在你的電腦上安裝防毒軟體是極其重要的。你可利用多數軟體程式提供的“自動更新”選項來保持最新的病毒定義檔，以確定它是最新的版本。永不打開任何人寄來的可疑檔案，除非你能百分之百地確定檔案內容、是誰寄的和為什麼寄給你。必要時，使用防毒軟體來檢查任何可疑的電子郵件附加檔案。

防毒軟體可以阻擋有害及危險的電腦病毒進入你的電腦和其他裝置，如：個人數位助理和行動電話。電腦病毒是一種軟體程式，任何特定病毒的實際作用，端視它是如何被設計和有什麼目的而定。有些病毒是蓄意設計來損害你系統上的檔案，或就某方面干擾你的電腦運作。所有的電腦病毒都可能會損害或毀壞儲存在你電腦硬碟裡的檔案。



一定要定期執行全系統病毒掃描。這些掃描可以在方便的時間自動執行。

警告： 多數使用者了解防毒軟體的需求且已在他們的電腦上安裝。然而，很多人忘記保持病毒定義檔在最新的狀態，這會使防毒軟體防護不完全。最好的防護是勾選“自動更新”的選項－這個功能會在你每次連上網際網路時，自動檢查最新的病毒定義檔。

在你的電腦上安裝反間諜程式 (Anti-spyware)

間諜程式是一個軟體程式，為了廣告、行銷的目的，在未經你的同意下，收集個人資訊或更改你電腦的配置。當你看到下列任何一種情形時，表示你的電腦上可能被安裝了間諜程式：

- 彈出廣告視窗，即使你並未連結到網際網路。
- 在你不知情的情形下，瀏覽器的首頁被更改了。
- 你的瀏覽器上多了新的工具列或其他你不記得曾安裝過的東西。
- 你的電腦好像運作緩慢，或使用比平常更長的時間來完成某些工作。
- 有些設定被更改了，而你無法將它們改回原有的設定。
- 在沒有任何明顯原因的情況下，電腦當機的情形增加。

一定要經常執行系統的間諜程式檢查來防止惡意的應用程式。如果不能每週執行，也應該每兩週執行一次。

警告： 每個反間諜程式都是被設計來尋找不同類型特定的問題，所以你應該安裝一個以上的反間諜程式。請聯絡不同的製造商，決定那種組合最符合你的需求。

備份你的資料

開發並遵循備份策略來保護你的資料。遺失檔案有太多原因，並非全都是肇因於安全性的問題，停電、硬體故障和人為錯誤都可能引起檔案遺失。最好的保護就是定期備份你的檔案。你需要決定備份的時間表、儲存裝置的種類和是否利用遠程備份裝置。

不管自己做或租用服務替你做，你需要決定備份的時間表和注意下列各點：

- 完整備份 :完整的備份包含所有數據和系統檔案。你通常不用每天做，因為你多數的檔案不會每天更改。
- 差異備份：從上次完整備份後有更改過的檔案。
- 增加備份：從上次備份後有更改過的檔案(不管是差異、增加或是完整備份)。這佔用的時間和儲存空間最少，但在資料遺失的情形下，你必須從幾個備份裡回復資料，且以正確的順序回復它們。

你可以備份至磁帶、CD、DVD或輔助硬碟。現在也有提供線上備份服務，或提供異地儲存器來更進一步保護你的資料免於實體災害(如：火災、洪水、偷竊、意外地刪除)。

警告： 對你的備份檔案做定期檢驗是很重要的。如果你不能在需要時用它來回復系統，那備份有什麼用呢?目前最好的方法是利用安全的線上儲存功能來存放你的備份檔案。這可以保護你的資料免於實體損害(如: 火災、洪水)和未授權的使用。

定期更新你的軟體

建議您利用“自動更新”選項更新軟體。如果你不保持更新的話，在你電腦上執行的軟體可能是安全性問題的一個來源。當程式使用一段時間後，會發現小問題，而製造商將需要設計”更新程式”或”修補程式”來解決它們。

此外，軟體程式的每一新版本，都應包含了新的安全性措施，因為聲譽好的軟體製造商會努力使線上環境更安全，而Windows、MAC或Linux等作業系統軟體廠商更是如此。你最要關注就是執行你的作業系統和所有應用程式的最新版本。

警告：“自動更新”選項是讓你的軟體保持最新版本的最佳方法，不過有些更新牽涉到較大的檔案。如果你是使用以資料量為基礎的網路方案，也許需要監控程式更新的情形，以避免超出下載量的限制。

不要打開電子郵件的附加檔案

在未確定電子郵件的來源前，切勿打開電子郵件的附加檔案。電子郵件地址是可以偽裝成讓寄件者看起來像是你認識或信任的人，因為多數的電腦病毒、蠕蟲和特洛伊程式是藉由電子郵件的附加檔案散播，最好的防護方式是在打開檔案前和寄件者聯繫一下。你也可以用你的防毒軟體來執行手動掃描附加檔案，以確定開啟它是否安全。

無線網路安全核對清單

當你設定無線網路時，你是否：

- ✔ ✘ 控制你的廣播區域? 第9頁
- ✔ ✘ 更改預設的密碼和使用者名稱? 第10頁
- ✔ ✘ 打開加密功能? 第10頁
- ✔ ✘ 小心且聰明的使用網路名稱(SSIDs)? 第10頁

給進階使用者

- ✔ ✘ 限制使用權利? 第12頁
- ✔ ✘ 驗證所有的使用者? 第13頁
- ✔ ✘ 限制使用者位址的數目? 第12頁

為保護你的電腦和個人資料，確定你：

- ✔ ✘ 將你的作業系統升級至最新版本。第22頁
- ✔ ✘ 設計 “堅固的” 密碼。第22頁
- ✔ ✘ 安裝個人防火牆。 第23頁
- ✔ ✘ 安裝防毒軟體。第24頁
- ✔ ✘ 安裝反間諜程式。 第24頁
- ✔ ✘ 定期備份。第24頁
- ✔ ✘ 升級所有應用程式至最新版本。第25頁
- ✔ ✘ 不要打開電子郵件附加檔案。第25頁

從公用的無線網路熱點使用網際網路前，你是否：

- ✔ ✘ 關閉 “檔案和印表機共享” 功能? 第14頁
- ✔ ✘ 關閉 “電腦對電腦 (點對點)傳輸網路”？第14頁
- ✔ ✘ 清除 “喜好的網路” 清單? 第14頁
- ✔ ✘ 檢查並確認你不是在傳送敏感性的資料? 第15頁
- ✔ ✘ 加密所有檔案? 第15頁

在用你的行動電話或個人數位助理來使用網際網路前，你是否：

- ✔ ✘ 安裝防火牆? 第17頁
- ✔ ✘ 安裝防毒軟體? 第17頁
- ✔ ✘ 設計一個 “堅固的” 密碼? 第17頁
- ✔ ✘ 開啟加密功能? 第17頁
- ✔ ✘ 當不使用時關閉藍芽? 第18頁
- ✔ ✘ 備份你的資料? 第16頁

為了不觸犯法律，請確定你：

- ✔ ✘ 沒有在未經明確許可下使用私人的無線網路。第20頁
- ✔ ✘ 沒有試圖私下使用其他私人無線網路使用者的資料。第20頁
- ✔ ✘ 沒有對任何私人網路上的資料和設定做任何未經授權的更改。第21頁
- ✔ ✘ 沒有在未經許可的情形下監看私人的無線網路。第20頁
- ✔ ✘ 保證你責任範圍內的任何無線網路能安全且有效地抵抗未經授權的使用。第21頁

連結

www.ieee.org	IEEE (美國電子電機工程師學會)是一個非營利、技術性的專業協會，在近175個國家擁有超過360,000位個人會員。
standards.ieee.org/wireless/	IEEE無線標準區域
www.wi-fi.org	Wi-Fi聯盟創立於1999年，是一個非營利、世界性的聯盟。證實以IEEE 802.11規格為基準的無線局部區域網路(LAN)產品，能讓軟硬體在多種品牌機器上做有意義的溝通。
www.apple.com/support/security/	蘋果電腦產品安全之網頁
www.microsoft.com/security	微軟資訊安全之網頁

致謝

當AOEMA的Michael Baker和Jan Gessin在編寫這本手冊時，很多人參與它的編輯，免費提供他們自己的時間和意見，尤其是下列政府的職員，在保證這份文件的準確性上扮演極其重要的角色：

- 澳洲政府
- 香港特別行政區政府，政府資訊科技總監辦公室
- 皇家泰國政府
- 美國政府

另外，來自私人企業和學術界的個人花費時間來複審這本手冊，我們想要感謝他們的貢獻：

- Nick Ellsmore – SIFT Pty Ltd (澳洲)
- Cynthia Kuo – Carnegie Mellon University
- Adrian Perrig – Carnegie Mellon University
- Craig Searle – SIFT Pty Ltd (澳洲)
- Dr Corey Schou – NIATEC, Idaho State University
- Rosemary Sinclair – International Telecommunications Users Group(INTUG)
- Richard Thwaites – Rich Communications
- Dr. Jesse Walker – 英特爾

Asia-Pacific Economic Cooperation
APEC 出版品 #205-TC-01.1
www.apec.org

www.aoema.org

FMMC (日本)
www.fmmc.or.jp

2005年3月

無線網路安全

在讀這本手冊時你需要知道什麼?

爲你的問題找尋答案

配置你的無線網路基地臺

使用公用的無線網路熱點

使用行動電話和個人數位助理

無線網路安全核對清單

本系列其他出版品

Safety Net www.aoema.org

網上安全

這本指引可助你提升「網上安全」

Safety Mail www.aoema.org

電郵安全

這本指引可助你在網上安全通訊

本小冊子為AOEMA所出版的Safety Wireless英文版的中譯本；
Safety Wireless英文原版刊載於網址：http://www.aoema.org/Safety Wireless/index.htm。
行政院研究發展考核委員會與國家資通安全會報技術服務中心獲AOEMA授權翻譯及出版本小冊子。
如對本小冊子的內容有任何查詢，請與國家資通安全會報技術服務中心連絡，連絡電話：(02)2739-9922。
This booklet is a Chinese translation of Safety Wireless published by AOEMA in English.
The original version of Safety Wireless can be found at http://www.aoema.org/Safety Wireless/index.htm.
[Research, Development, and Evaluation Commission, Executive Yuan] and [Information & Communication Security Technology Center] have obtained the approval of AOEMA to translate and publish this booklet.
For enquiries about the contents of the translation, please contact us as (02)2739-9922.

行政院研究發展考核委員會
Research, Development, and Evaluation Commission, Executive Yuan

ICST 行政院國家資通安全會報技術服務中心
INFORMATION & COMMUNICATION SECURITY TECHNOLOGY CENTER

ISBN : 0-9757398-2-4