

# 無線網絡的保安

2010 年 12 月

© 香港特別行政區政府

這份文件的內容為香港特別行政區政府的財產，未經香港特別行政區政府的明文批准，不得轉載全部或部份文件內容。

**免責聲明：**政府盡力確保本文資料準確，但不明示或隱含保證資料準確無誤。對於因使用本文資料而引致或與之有關的任何錯誤或遺漏，香港特別行政區政府概不承擔任何法律責任。

## 目錄

摘要 .....	2
I. 無線網絡簡介 .....	3
無線局部區域網絡 .....	3
無線接駁點.....	3
服務設定識別碼 .....	3
開放式系統認證（Open System Authentication） .....	3
分享式密碼匙認證（Shared Key Authentication） .....	3
臨機操作模式（Ad-hoc mode） .....	4
基建模式（Infrastructure mode） .....	4
有線等效保密規約（Wired Equivalent Privacy（WEP）） .....	4
Wi-Fi Protected Access 和 Wi-Fi Protected Access 2.....	4
II. 保安威脅及風險 .....	6
停車場攻擊（Parking lot attack） .....	6
分享式密碼匙認證瑕疵.....	6
服務設定識別碼（SSID）的瑕疵.....	7
有線等效保密規約的漏洞.....	7
暫時密碼匙完整性規約（TKIP）攻擊.....	7
III. 機構環境中是否可使用無線網絡作資訊處理.....	8
IV. 機構推行無線網絡的最佳作業實務.....	9
推出階段.....	9
設計／採購階段 .....	9
實施階段.....	11
操作及維修保養階段 .....	12
棄置階段.....	13
V. 使用無線網絡的最佳作業實務.....	14
在家裡配置無線寬頻路由器的貼士 .....	14
使用公共無線服務瀏覽互聯網的貼士 .....	15

## 摘要

現今科技一日千里，在無線設備的價格相宜及效能提升的情況下，很多辦公室和公共地方都已安裝無線設施。本文將討論無線網絡的保安威脅及風險，並且在企業和家居環境建立無線網絡方面提供最佳作業實務。最後，更會為終端用戶提供使用公共無線網絡瀏覽互聯網時的保安貼士。

## I. 無線網絡簡介

無線互聯網接達技術在辦公室和公共環境，甚至家居互聯網用戶中日漸普及，以下將介紹一些無線網絡系統的基本技術。

### 無線局部區域網絡

無線局部區域網絡（WLAN）是一種利用高頻無線電波（而非經線路）在啟動了網絡功能的裝置之間進行通訊的局部區域網絡。

### 無線接駁點

無線接駁點（AP）是一個硬件裝置，讓無線通訊裝置如 PDA 及手提電腦連接無線網絡。通常 AP 連接有線網絡是爲了提供一個橋路（bridge），使有線和無線裝置之間的數據得以傳輸。

### 服務設定識別碼

服務設定識別碼（SSID）是可設定的識別碼，無線客戶端可憑識別碼跟適當的無線接駁點通訊。只要配置正確，客戶端擁有正確的 SSID 便可以與無線接駁點通訊。此外，SSID 還可以作爲無線接駁點及客戶端之間的單一分享密碼。

### 開放式系統認證（Open System Authentication）

開放式系統認證是 802.11 標準的預設認證規約，包含了簡單的認證要求，內有工作站 ID 和含有成功或失敗數據的認證應答。成功認證後，兩台工作站已互相認證。該認證亦可配合 WEP（有線等效保密規約）一併使用以提供較安全的通信渠道，但須注意在認證過程中認證管理框仍是以純文本傳送的，唯認證過程完成後 WEP 才會對數據進行加密。任何客戶端均可傳送其工作站 ID 嘗試聯繫無線接駁點，造成沒有實際地進行認證的效果。

### 分享式密碼匙認證（Shared Key Authentication）

分享式密碼匙認證是採用 WEP 和分享式密碼匙的標準質疑應答機制，用於提供認證。WEP 使用分享式密碼匙替質疑文本加密，認證客戶端將加密質疑文本送回無線接駁點

以作出確認。如果無線接駁點能夠解密出相同的質疑文本，即表示認證成功。

### **臨機操作模式 (Ad-hoc mode)**

臨機操作模式是 802.11 標準的網絡布局之一，包括至少兩台無線工作站的通訊，而不包括無線接駁點。由於不需要無線接駁點作通訊橋樑，臨機操作模式的 WLANs 相對地較便宜。這種布局不適用於大型的網絡，而且該模式亦缺乏了部份保安功能，如 MAC 地址過濾和訪問控制。

### **基建模式 (Infrastructure mode)**

基建模式是臨機操作模式以外另一種 802.11 標準的網絡布局，包括多台無線工作站和無線接駁點。無線接駁點通常連接到較大的有線網絡，其網絡布局可擴展至覆蓋率多樣化及較複雜的大型網絡。

### **有線等效保密 (Wired Equivalent Privacy (WEP))**

有線等效保密 (WEP) 規約是 IEEE802.11 標準的基本保安功能，可在無線網絡中替傳輸資料進行加密，提供保密性。WEP 密碼匙的 key-scheduling 弱點已被發現，WEP 密碼匙已可被自動破解工具於數分鐘內破解。因此，如非沒有其它較安全的選擇，否則不應選用 WEP。

### **Wi-Fi Protected Access 和 Wi-Fi Protected Access 2**

Wi-Fi Protected Access (WPA) 是針對 WEP 的缺陷而設計的無線保安規約。WPA 能為用戶提供較高的保證，例如用戶的數據可透過暫時密碼匙完整性規約 (TKIP) 進行數據加密後得到保護，並且引進了 802.1x 認證技術為用戶提供最佳的認證過程。

Wi-Fi Protected Access 2 (WPA2) 是依據 IEEE802.11i 標準的嶄新無線保安規約，只有獲授權的用戶才可接達無線裝置，並支援更強的加密法 (高級加密標準 AES)、更強的認證控制 (可擴展認證規約 EAP)、密碼匙管理、中繼攻擊保護和數據完整性的功能。

有安全廠商在 2010 年 7 月，聲稱發現了名為 "Hole 196" 的 WPA2 安全漏洞。據說此漏洞容許已進行內部認證的 Wi-Fi 用戶，可解密其他用戶的數據，及注入惡意數據到無線網絡上。經調查後<sup>1</sup>，此漏洞實際上並不能恢復、破壞或拆解任何 WPA2 的加密金鑰 (AES 或 TKIP)。攻擊者只能偽裝成無線接駁點，待客戶端連接到他們時，

---

<sup>1</sup> 分析 WPA2 "Hole 196" 攻擊。

(<https://airheads.arubanetworks.com/article/aruba-analysis-hole-196-wpa2-attack>)

才能發動中間人攻擊。此外，只要系統的配置適當，該攻擊是不會成功的。假如接入點已啓用了客戶端隔離功能，無線用戶便不能在同一個接入點互相交談，這樣攻擊者亦無法對無線用戶發動中間人攻擊。

TKIP 多會配合 WPA 使用，而較強的 AES 加密算法則會配合 WPA2 一起使用的。有些設備能允許 WPA 與 AES 一併使用，而另外一些設備則可允許 WPA2 與 TKIP 一併使用。但 TKIP 在 2008 年 11 月被發現存在漏洞，它可讓攻擊者解密網絡上的小封包並注入任意數據到無線網絡中。因此 TKIP 加密不再被視爲一個安全的方案，在架建新的無線網絡時應該考慮使用安全性較高的 WPA2 規約並以 AES 加密。

## II. 保安威脅及風險

推行無線網絡的成本較低，因此極受歡迎。雖然低廉的成本是無線網絡極具吸引力的賣點，但廉宜的設備也令攻擊者更容易發起攻擊。802.11 標準的保安機制在設計上的瑕疵也引發了一連串被動和主動攻擊，導致無線傳輸的資訊被竊聽及遭竄改。

### 停車場攻擊 (Parking lot attack)

無線接駁點以循環形式傳輸訊號，而這些訊號幾乎總會延伸到預定覆蓋的工作地點實體界限以外。這些訊號可能在建築物外，或甚至在穿過多層大廈的地台時被截取。攻擊者便能夠藉此發起停車場攻擊，攻擊者可安坐在機構的停車場，嘗試通過無線網絡接達內部主機。

如果網絡安全措施被破解，攻擊者便等於入侵到了網絡的其中一個關鍵部份。攻擊者的入侵穿過了防火牆，並具有與機構可信賴員工一樣的網絡接達權限。

攻擊者還可在附近地點設置未經授權的無線接駁點，向鄰近的真實無線客戶發出更強烈的訊號，以誘騙他們連接攻擊者自己的網絡，從而在他們嘗試登入這些假冒的伺服器時，騙取他們的密碼和類似的敏感數據。

### 分享式密碼匙認證瑕疵

透過竊聽無線接駁點和認證客戶端之間的質疑及應答，共享密碼匙認證便可輕易被這種被動攻擊所破解。這種攻擊是可行的，因為攻擊者可收集純文本（質疑）和加密文本（應答）均已洩露。

WEP 採用 RC4 串流加密作為加密算法。串流加密以產生密碼匙串流（即根據共用密碼匙和初始向量 (IV) 產生一連串偽隨機數元）來加密。密碼匙串流對照純文本被 XORed，以產生加密文本。串流加密的一大特點是如果純文本和加密文本均被洩露，只需要簡單地 XORing 純文本和加密文本，便能夠將密碼匙串流復原，在上述情況下即復原質疑應答。被復原的密碼匙串流會被攻擊者利用，將無線接駁點其後產生的任何質疑文本加密，通過一併 XORing 兩個數值，作出有效的認證應答，攻擊者從而通過無線接駁點認證。

## 服務設定識別碼 (SSID) 的瑕疵

無線接駁點提供預設的 SSIDs。如果不修改這預設值，這些配置不當的設備便較易招引攻擊者下手。此外，即使無線接駁點已設定為不廣播 SSIDs 或啓動加密，管理封包中仍包含 SSIDs，並在大氣中以純文本方式傳送。攻擊者只要截聽和分析無線網絡通訊，便能夠收集 SSID 以作進一步攻擊。

## 有線等效保密規約的漏洞

大部份 WLAN 產品的 WEP 功能都預設為關閉狀況，用戶使用無線網絡傳輸數據時便很容易被竊聽，並遭到竄改數據的攻擊。然而，即使啓動 WEP 功能，無線通訊的保密性和完整性仍備受威脅，因為有研究顯示，WEP 存在不少瑕疵，嚴重影響了 WEP 聲稱的保安功能。WEP 可能特別遭受下列攻擊：

1. 利用已知道的純文本和選定加密文本攻擊，從而將通訊解密的被動攻擊;
2. 對加密文本進行統計分析，從而將通訊解密的被動攻擊;
3. 由未獲授權的流動站點加入新通訊的主動攻擊;
4. 竄改數據的主動攻擊; 或
5. 蒙騙無線接駁點，使它向攻擊者的電腦轉發無線通訊，從而將通訊解密的主動攻擊。

## 暫時密碼匙完整性規約 (TKIP) 攻擊

TKIP 攻擊是使用了類似 WEP 攻擊的手法，攻擊者試圖每次只對一個字節進行解碼並監測回放該字節到網絡後的反應。利用這種方法，攻擊者只需約 15 分鐘便可以對網絡上的小封包如 ARP 封包成功解碼。假如網絡是啓用了服務質量 (QoS)，攻擊者更可以進一步注入高達 15 組任意數據到已解密的封包中。潛在的攻擊包括 ARP 下毒、域名系統操縱及拒絕服務等。

雖然這不是一個針對解密金鑰的攻擊及不會導致所有 TKIP 加密封包遭解密，但仍然會對所有採用 TKIP 加密方法的 WPA 和 WPA2 網絡構成風險。

### III. 機構環境中是否可使用無線網絡作資訊處理

近年來，使用無線網絡的機構數字上升，很多中小企業（SMEs）轉為使用無線網絡，原因是無線裝置的成本低，使用時又方便，就算大機構亦考慮廣泛推行無線網絡<sup>2</sup>。然而，方便與彈性是有代價的，無線網絡規約本身的特點和弱點令其在使用時的保安威脅提高。因此，有必要檢視在機構環境中，是否適合使用無線網絡作資訊處理用途。

首先，是否可使用無線網絡可根據資訊傳輸的不同而分類，例如香港政府內部已經就是否可使用無線網絡發出指引。以下列表根據保安條例的要求而將資訊傳輸作出分類，從而概括無線網絡的應用性。

資料類別	是否可使用無線網絡傳輸資料
絕對機密	不可使用
高度機密	不可使用
機密	可使用，但必須有足夠的認證和傳輸資料加密保安控制，並達到機密資料必須達到的加密水平。 宜使用虛擬私有網絡（VPN），以加強無線局部區域網絡連接的認證和加密功能。此外，亦須制定適當的密碼匙管理及配置政策，以輔助技術方案。
限閱	可使用，但必須有足夠的認證和傳輸資料加密保安控制，並達到限閱資料必須達到的加密水平。 宜使用機密資料必須達到的同一加密水平，並制定與機密資料相似的適當的密碼匙管理及配置政策。
非機密	可使用。遵循只有獲授權人士才允許接達儲存資料的網絡的原則，且具備足夠及適當的認證和傳輸資料加密措施的無線網絡才可用於政策局／部門。 與機密及限閱資料一樣，亦須制定適當的密碼匙管理及配置政策，以輔助技術方案。

<sup>2</sup> <http://www.entrepreneur.com/tradejournals/article/162337616.html>

## IV. 機構推行無線網絡的最佳作業實務

使用無線網絡可帶來成本效益及方便，令它在大小機構中的應用日趨普遍。無線網絡的應用雖然有不少好處，卻同時帶來新的保安風險。要有效地減低這些風險，在無線網絡方案的整個發展周期中，應考慮各種保安最佳作業實務。為協助機構了解在無線網絡推行期間的最佳作業實務，我們會以一個分為五個階段的網絡發展周期作為基礎，逐步指出保安方面需要特別注意的重點。

### 推出階段

#### 就使用無線網絡釐定業務及功能的需求

在設計無線網絡前，須了解無線方案業務及功能的需求，因為這些需求可能會影響應採取的網絡保護措施。例如，倘若容許非註冊用戶接達系統，在設計階段便應考慮相關的最佳保安作業實務。

#### 訂立無線保安政策

機構應制訂一套穩健的無線保安政策，以處理使用無線網絡的問題及釐定可傳送的資料種類。該政策應描述一個制訂安裝、保護、管理和使用程序的架構，以及訂立保安與運作指引、標準和各員工的職責。

### 設計／採購階段

#### 留意 Wi-Fi 標準的發展

自從 802.11 標準推出並不斷加以改良，數據傳輸率、訊號範圍和無線網絡的保安都得以加強，因此，當採購新設備或獲取新的無線網絡服務時，最好時常留意新標準的發展。在採購新設備時，應考慮以較安全的無線保安規約如 WPA/AES 或 WPA2/AES 作保護。由於日後可能在這些規約中發現新的保安漏洞，故不能只依賴這些保安規約作為確保資料保密性和完整性的唯一措施。

#### 進行保安風險評估及審計以識別保安漏洞

保安風險評估及審計是必要的方法，用以查核無線網絡的保安情況，並確定所需的修正

措施以維持可接受的保安水平。保安風險評估有助於識別無線網絡的漏洞，例如無線接駁點使用預設配置，或容易猜透的密碼和 SNMP 暗號，以及是否有加密功能等。然而，保安風險評估只能揭示資訊系統於某一段時間的部份風險，因此在無線網絡投入運作後，應定期進行評估及審計。

## 進行實地調查

基於射頻 (RF) 的性質，無線網絡訊號一般不會受樓宇阻隔。無線訊號的覆蓋範圍過大，可能會對網絡構成重大威脅如停車場攻擊。因此，在網絡策劃階段中，應充份了解無線網絡的覆蓋範圍要求並進行實地調查，以便確定：

1. 適宜採用的技術；
2. 須避免、清除或處理的障礙；
3. 應採用的覆蓋模式；及
4. 需要的容量

## 採用縱深防禦方式

有線網絡的保安設計，一直廣泛採用「縱深防禦」的概念，這原理亦適用於無線網絡。經採取多重保安措施後，無線網絡遭成功入侵的風險將大幅減少。如一項措施受襲，尚有多重保安措施可保護網絡。

分隔無線與有線網絡數據段、使用強化的裝置及用戶認證方法、依據位址及規約作出網絡過濾，以及對無線與有線網絡進行監視和入侵偵測，均是多重防禦的措施。

## 分隔無線網絡與有線網絡

基於無線技術的特質，無線網絡比較難以受樓宇阻隔，故一般被視為不可靠的網絡。連接網絡時，最佳的作業實務是有線和無線網絡不應直接連接在一起。防火牆的安裝通常用於分隔和控制不同網絡的通訊。譬如，有線網絡的 ARP 廣播封包不應傳送至無線網絡，否則惡意用戶便可揭露內部信息，例如這些廣播的以太網 MAC 位址。

## 無線接駁點的覆蓋範圍分段

由於無線網絡的傳送容量有限，惡意攻擊者可輕易進行拒絕服務 (DoS) 攻擊，使網絡停頓。把無線接駁點的覆蓋範圍分段，可平衡無線網絡的負荷，並減少 DoS 攻擊的影響。

## 實施階段

### 推行有效的實體保安管制

網絡設備的遺失可能會對無線網絡構成重大威脅，因為網絡的配置可從遺失的無線接駁點或無線界面卡中取得。把網絡設備如無線接駁點安全地放置在不容易接觸的位置，並加設有效的實體保安管制，被竊的風險便會減少。

### 避免無線網絡的覆蓋範圍過大

從實地調查收集資料後，便可設計放置無線接駁點的位置，以免無線網絡的覆蓋範圍過大，因而減少遭入侵的機會。此外，調較傳送的射頻功率（RF）或使用定向天線，亦可控制傳送的射頻訊號，從而控制無線網絡的覆蓋範圍。

### 保障無線接駁點的安全

無線接駁點是無線網絡的核心，它們是否安全，對無線網絡的整體保安有一定的影響。要保護無線網絡，首先要確保無線接駁點的安全。以下是加強管理無線接駁點安全的一些建議：

1. 更改配置的預設值；
2. 定期更換密碼匙；
3. 確保所有無線接駁點均有安全而獨立的管理密碼，並定期更換密碼；
4. 關閉無線接駁點上所有不安全及未使用的管理規約，並以最小權限配置餘下的管理規約；
5. 啓動記錄功能，並把記錄傳送至遠程記錄伺服器；
6. 啓動無線基本參數，例如靜止逾時及支援結合上限。

### 使用難以聯想到的服務設定識別碼（SSID）命名常規

無線網絡中，SSID 用作分段網絡的網絡名稱，客戶端須配置正確的 SSID 才能接達網絡。SSID 值會顯示位標、探測請求及深測回應廣播，因此，為免惡意攻擊者在無線網絡裝置竊取偵察資料，SSIDs 不應反映機構的內部資料。

### 關閉客戶端與客戶端之間的「臨機操作模式」傳送功能

一般而言，無線網絡可透過三種不同方式運作：基建、臨機操作及橋路模式。利用臨機操作模式運作時，客戶端之間可直接連接而不同無線接駁點。如客戶端配置不善，攻擊

者不費吹灰之力便可接達客戶端。因此，除非有特別的業務需要，否則應關閉無線裝置的臨機操作模式。

### **限制客戶端與客戶端之間透過無線接駁點的通訊**

大部份無線網絡以「基建」模式運作，需要使用一個或以上無線接駁點，所有網絡交通均穿越無線接駁點。透過控制無線接駁點的客戶端通訊，可防止惡意用戶接達易受破壞的客戶端。

### **保持最新的保安修補程式**

電腦產品新發現的保安漏洞應即時修補，以免受到無意或惡意的攻擊。修補程式在使用前亦應先進行測試，以確保能有效運作。

### **在無線接駁點實施 MAC 位址過濾**

MAC 位址過濾可視作無線網絡的第一層保護。啟動過濾功能後，只有獲授權的裝置才可使用網絡。由於互聯網上有工具可修改 MAC 位址，故不可單靠這種接達控制方式來保護數據的保密性和完整性。此外，MAC 位址過濾機制在一些情況下並不適用，例如實施公共無線熱點的時候。

### **採用無線入侵偵測系統**

在網絡上採用無線入侵偵測系統，有助及時偵測惡意破壞活動和作出回應。現時，一些無線入侵偵測系統更備有可偵測及預防非法無線接駁點的功能。

### **操作及維修保養階段**

#### **教育用戶無線技術的風險**

用戶知悉風險所在，往往是確保資訊保安的成功關鍵。完善的政策並不足夠，教育用戶遵行政策同樣重要，故應訂定最佳作業實務或保安指引，讓終端用戶了解和跟隨。

#### **備存所有無線裝置的詳細清單**

一份準確的獲授權使用的無線裝置清單，有助於在保安審計時確定非法的無線接駁點，以及進行不同的支援工作。

## 公布無線網絡的覆蓋圖

網絡管理員應建立無線網絡的覆蓋圖，包括各無線接駁點的位置和 SSID 資料。當發生保安事故，這覆蓋圖對於解決問題將會起很大的作用。

## 訂立無線接駁點的保安配置標準

為簡化日常工序，並確保各無線接駁點受適當的措施保護，建議為無線接駁點訂立基準保安配置標準。當無線接駁點運作故障，常見的做法是將其重設到預設值。如訂立了基準保安配置標準，有關人員只需要按照標準便可重新配置無線接駁點。

## 定期檢查審核記錄

機構必須定期檢查審核記錄，以確保記錄齊全完整。如發現不尋常情況必須作出匯報，並且有需要時應進行詳細調查。

## 訂定保安事故應變程序

建議管理員訂定一套內部保安事故應變程序，以及不時更新以處理新的潛在保安威脅。

## 棄置階段

### 棄置裝置前刪除所有敏感資料

在棄置無線組件時，緊記刪除裝置上所有的敏感配置資料，例如共享密碼匙和密碼。如惡意用戶取得這些資料，便可用作攻擊網絡。因此，在棄置裝置前必須透過管理界面以人手刪除配置設定。機構可考慮在可行情況下為設備消磁，如有硬磁碟裝置，亦可使用安全刪除工具。

## V. 使用無線網絡的最佳作業實務

### 在家裡配置無線寬頻路由器的貼士

#### 如何選擇我的無線網絡模式？

一般而言，無線網絡可透過三種不同方式運作：基建、臨機操作及橋路模式。利用臨機操作模式運作時，客戶端之間在沒有無線接駁點下可直接連接。如客戶端配置不善，攻擊者不費吹灰之力便可接達客戶端。因此，除非有特別的業務需要，否則應關閉無線裝置的臨機操作模式。

#### 如何安全放置我的無線寬頻路由器？

1. 避免把路由器放置近牆壁或窗口，亦盡量不要放在貼近隔壁的位置，以確保訊號不會超出所需範圍。
2. 把路由器實體放置在安全的地方，以確保不會被未獲授權人士竄改。
3. 一些路由器可讓你減低裝置的輸出能量，可以的話，應調低廣播能量以減少無線網絡服務的覆蓋範圍。這方法可防止過強的訊號超出理想的無線廣播範圍，而使外界可接達網絡。

#### 如何安全配置我的無線寬頻路由器？

##### 用戶名稱及密碼

更改預設的用戶名稱及密碼，因為預設值往往容易被猜出來。一些製造商未必讓您更改使用戶名稱，但至少應可更改密碼。

##### 加密（WEP/WPA/WPA2）

應盡量避免使用 WEP。假若裝置能支援的話，應使用 WPA2/AES 或 WPA/AES。

##### 認證種類（開放式認證或共享式密碼匙認證）

絕不採用共享式密碼匙認證。應考慮採用 802.11i 標準中訂立的強化相互認證。

## 無線網絡名稱／SSID

更改預設的 SSID。新的 SSID 不應以使用中的網絡產品、自己的名字或其它個人資料命名，否則該 SSID 將有助攻擊者收集有關你和你所使用的無線網絡的資料。

## 廣播網絡名稱／SSID

用戶應關閉 SSID 廣播，或增加「Beacon Interval」至最大值。關閉或減低 SSID 廣播，雖然不能防止進階黑客從無線接駁點與客戶端通訊的管理封包中竊取 SSID，卻可避免一般無線用戶發現該無線網絡的存在，或嘗試訪問它。

## MAC位址過濾

建議啓動 MAC 位址過濾作為另一層保護。

## 動態主機配置規約（DHCP）

盡量關閉 DHCP 功能，因為 DHCP 容易讓惡意攻擊者接達無線網絡。

## 使用公共無線服務瀏覽互聯網的貼士

當無線裝置（例如手提電腦或手提裝置）接達公共無線熱點，便有機會受遠程攻擊者的威脅。雖然如此，以下的保安貼士可以助你遠離攻擊者的陷阱：

1. 切勿隨意擺放你的無線裝置而不加看管；
2. 以密碼保護裝置：啓動裝置的開機登入功能、系統登入身份認證和設有密碼的屏幕保護。
3. 如沒有需要，關閉無線連線：當無線裝置啓動了 Wi-Fi、紅外線及藍芽，便會經常對外發出訊號，等於在你不知不覺間向攻擊者招手。
4. 使用最新的無線網絡界面卡驅動程式：網絡界面卡只是一般軟件，並非萬毒不侵。因此，要經常更新最新的驅動程式，以確保無線裝置從產品供應商得到最新的保護和支援。
5. 以含有最新病毒定義的防毒軟件來保護裝置，可減低感染電腦病毒或間諜軟件的風險。
6. 替裝置上的敏感／個人資料加密：就算當未獲授權用戶成功接達裝置，經加密的資料對竊匪來說已加多一重障礙。
7. 關閉無線界面卡的資源共用規約：當共享檔案和文件夾時，可能會吸引攻擊者試圖操控共享的資源。
8. 使用公共無線服務時刪除你的「慣用網絡」：有些操作系統會讓你把一些常

用的無線網絡設定為「慣用網絡」，一經設定，你的系統會不斷尋找並嘗試自動連接這些「慣用網絡」。通過收集由系統傳送出來的資料，攻擊者便可根據「慣用網絡」的無線網絡設定，設置一個虛假的無線接駁點。這樣，你的裝置便會自動連接到攻擊者虛假的無線網絡。

9. 關閉隨機操作模式網絡：「隨機」操作模式網絡以最低限度的保安對抗未獲授權的進入連接，讓你的無線裝置通過無線連接與其它電腦或裝置通訊。應關閉隨機操作模式以防止攻擊者容易接達在你裝置上的資料和資源。
10. 不要同時啟動無線及有線網絡界面卡：當無線網絡界面卡並未被關閉，而你的無線裝置連接到有線網絡，攻擊者便有機可乘地利用已啟動的網絡橋路並通過開放的無線網絡入侵有線網絡。
11. 檢查「捕獲門戶」(captive portal) 網站的真確性：「捕獲門戶」網頁常用於公共熱點作為用戶認證及阻嚇攻擊者的機制。當連接到公共熱點時，用戶會先被導向至「捕獲門戶」的網頁。然而，攻擊者也可以設立虛假的「捕獲門戶」網頁，藉此收集用戶的個人資料。所以，當連接到公共熱點時，用戶應先檢查「捕獲門戶」網站的伺服器證書以確定網站的真確性。
12. 切勿透過公共無線網絡傳輸敏感／個人資料：公共無線網絡通常被視為不安全的網絡，如沒有適當的保安控制，不應於公共無線網絡傳輸敏感或個人資料。
13. 採用虛擬私有網絡 (VPN) 加密無線通訊：如無可避免要在公共無線網絡傳輸敏感或個人資料，可採用虛擬私有網絡加密無線通訊以確保通訊的保密性。如要得到更多 VPN 技術的資料，請參考「虛擬私有網絡保安」一文。
14. 使用 VPN 時關閉分隔隧道功能：如果用戶已通過虛擬私有網絡連接私有網絡，同時又利用分隔隧道功能連接互聯網或其它不安全的網絡，這可能對所連接的私有網絡構成威脅。
15. 在棄置無線裝置前刪除所有敏感的配置資料：在棄置舊的無線裝置前，應先刪除所有敏感的配置資料，例如服務設定識別碼 (SSIDs) 或密碼匙。

當你使用公共無線網絡時，可根據上述的保安貼士去保護你的無線裝置和個人資料。雖然還有其它可採取的防範措施，但這些保安貼士不失為一個不錯的起步點。