

## 「熱點」無線上網，代價豈只一杯咖啡？

若你已採取一切措施妥善保護公司的網絡，設置堅固的防火牆，又時刻更新保安策略，甚至為分公司提供保安防護，那就會萬無一失嗎？沒錯，但就要你的員工從來不在咖啡店等「熱點」上網，登入它們的Wi-Fi連接。

其實大部分用戶都不知，一旦在這些地方無線上網，便會成為網上用戶群中一員。這用戶群從無線網絡接入點傳送的訊息，往往是很難控制的。用戶若不好運，很容易受到身旁用戶搭上的病毒和蠕蟲感染。染了網上病毒的用戶重返工作崗位後，局面便會一發不可收拾。如用戶把無線電子工具連繫到公司無線網絡接入點，嘆咖啡時在網上感染到的蠕蟲瞬即便會侵入企業網絡，帶來的損失可比最令人側目的java失誤更嚴重。公司還要派IT管理人員清理網絡。這亦是無線上網的代價。

現時無線上網熱點現已遍布世界各地的餐廳、酒店與機場；香港的餐廳、咖啡室、購物中心、辦公大樓等，無形中亦可能成為員工的「危險熱點」。方便易用的無線上網熱點帶來網絡保安危機，實在不容忽視。然而，所有為無線上網而定的保安標準卻未能提供以內容為基礎的保障，用戶必須自行防護。

現時的無線保安標準如 Wired Equivalent Privacy (WEP) 與 Wi-Fi Protected Access (WPA)，主要透過加密技術來關注

無線連接的私隱，確保只有經授權用戶才可憑藉身份核實，連接至無線網絡接入點。話雖如此，用戶身份獲核實，並連接至無線網絡登入點後，即使無線渠道設有加密功能，也容易把內容威脅由公司的防火牆等周邊防衛，傳送至無線網絡。

安全可靠的 WLAN 能有效防護任何人士無經授權登入連結、網絡，以及用戶與應用層。而安全可靠的無線平台則應涵蓋：1. 提供可靠的物理層連接與偵察接入點的機制；2. 禁止客戶終端之間不良的網絡層連接；3. 於應用層面提供惡意碼防護；4. 阻止任何人擅自使用網絡資源。

要設立以上所有保安屏障聽起來絕不簡單，但可採取不同的方式，是從教育入手，員工應當認識登入無線網絡的潛在保安危險。另外，不同的保安層，不管是設於網閘、內部伺服器及個別客戶機/終端，均須提供完善保護。這些技術需要提供身份核實與加密，偵察與清除內容威脅外，更需絲毫無損網絡效能。公司也必須確保各企業用戶的手提電腦備有有效的終端保安。

此外，於企業網絡邊緣檢查電郵與網上流量的無線防毒網閘與內部防護系統，可增置額外的保安層。萬一網上入侵透過周邊設備而來，網絡保安方案也能避免其肆虐破壞。