

家庭網路安全防護：如何保護路由器與選擇安全的網路設備

家庭網路安全並不只是為家中的 Wi-Fi 設定密碼那麼簡單。您的家人會在電視上觀看節目、線上購物、透過遊戲機連線，或在家工作。各種重要資料（身份資訊、密碼、地址、私人照片等），都會透過家庭網路持續連接至網際網路。

最常見的就是「網路釣魚」與「惡意軟體」等手法，駭客與病毒會利用這些手段偽裝自己，入侵家庭網路並竊取私人資訊。家庭網路安全是保護家人免受惡意攻擊的基礎，本文旨在幫助您了解基本安全知識並提升網路防禦等級。

如何保護您的路由器

通常，家庭網路由路由器和若干連接設備組成。路由器負責家庭網路與網際網路之間的資料傳輸，是抵禦外部攻擊的最重要防線。想讓路由器更難被入侵，可以進行以下設定：

1. 設定強效且唯一的管理員與 Wi-Fi 密碼

切勿使用預設密碼。駭客會利用公開的預設憑證嘗試入侵，定期更換密碼是維護安全的良好習慣

2. 保持韌體更新

最新韌體包含安全修補程式與漏洞修復。選擇支援自動更新的路由器，並確保該功能已啟用

3. 建立獨立的訪客網路

訪客網路與家庭主網路隔離，訪客可存取網際網路但無法存取您的私人資料

4. 停用 UPnP 功能

UPnP（通用即插即用）雖然方便，但容易被惡意軟體或不法分子利用來取得存取權限。停用這些功能能提供更嚴密的保護

如何選擇一款安全的路由器

1. 選擇支援 WPA3 加密協定的路由器

WPA3 是最新一代 Wi-Fi 安全協定，提供更強大的密碼加密，能有效抵禦暴力破解攻擊。若設備不支援 WPA3，選擇 WPA2/WPA3 混合模式也是個很好的選擇

2. 選擇具備內建安全機制與防護功能的路由器

現代路由器多內建網路安全服務，可防止惡意入侵、主動攔截威脅並修復網路漏洞

3. 使用具備 App 管理功能的路由器

透過Cudy手機 App 管理網路，能即時監控連線狀態。當發生異常連線或需要設定時，讓您也能遠端設定設備

如何保障家人上網安全

1. 設定孩子上網時長

透過家長監護功能管理每日上網時間，設定定時斷線或宵禁時間，協助孩子養成健康的數位習慣

2. 屏蔽有害與不當內容

利用內容過濾機制，阻擋白名單外或黑名單內的網址

3. 保護您的物聯網 (IoT) 設備

智慧攝影機與家電在遭遇外部入侵時容易暴露漏洞。為物聯網設備提供專屬安全防護，能避免私密畫面或資料外洩

輕鬆掌控您的家庭網絡：Cudy 解決方案

若您正在尋找兼具安全與效能的家庭網路方案，Cudy 全系列路由器與 Mesh 系統 是最佳選擇：

Cudy Mesh 全屋覆蓋與自動安全更新

Cudy Mesh 系統能以單一 SSID 實現無縫全屋涵蓋，同時支援最新的 WPA3 加密協定，並提供自動韌體更新功能，確保網路時刻具備最新安全防護

進階家長監護與安全防護

透過 Cudy App，您可以輕鬆設定家長監護功能、排定上網時間、過濾不當內容，並即時管理連線裝置

IoT 設備隔離與訪客網路

Cudy 路由器支援快速設定獨立的訪客專用網路，將訪客設備與您的核心個人資料完全隔離，降低風險

常見問題 Q&A

Q：所有 Cudy 產品都支援 WPA3 與 Mesh 功能嗎？

答：Cudy 路由器目前除了 LT300 以外，均完整支援 Cudy Mesh 技術。WPA3 則是全數 Cudy 的路由器皆支援

Q：如何更新 Cudy 路由器的韌體？

答：您可以在 Cudy App 中直接檢測並開啟自動更新，或至碩鋒官方下載中心（[點我至下載中心](#)）下載最新韌體進行手動更新

Q：關閉 UPnP 會不會影響 PS5、Switch 或智慧家電的連線？

答：關閉 UPnP 可能會使部分遊戲機的 NAT 類型變為 Strict（嚴格）。若遇到連線問題，建議透過 Cudy 管理介面針對特定裝置設定「單一埠轉發」，兼顧安全與連線品質

Q：如果設定了高強度密碼後忘記管理員密碼，該如何處理？

答：可長按 Cudy 路由器的 Reset 重置鍵約 5 秒，看到燈號快速閃爍後放開恢復出廠設定，再使用預設密碼重新設定

Q：如何防範惡意網站與 DNS 劫持攻擊？

答：Cudy 支援自訂 DNS，如 Cloudflare、Quad9、Google，以及 DNS over TLS (DoT) 加密技術，能防止 ISP 或第三方綁架您的網址查詢，確保瀏覽安全