SAMSUNG

Knox 實用秘笈：Galaxy 如何隨時隨地默默守護裝置安全

Galaxy 透過「自動封鎖程式」、「Message Guard」及「安全更新」助用戶抵禦網路威脅並掌控裝置隱私

幾乎每天都會出現影響消費者、企業和組織的網路安全威脅消息，而這些威脅可能在網路、資料和裝置內部形成風險，相關事件一旦發生即呈指數級增長。使用者知道這些威脅會以惡意軟體或釣魚攻擊等多樣型態出現，但當受害者察覺時，通常為時已晚。

強大的 Galaxy 安全解決方案提供多種方法來保護裝置安全並協助用戶掌控個人隱私，有效遠離網路安全威脅。其中，「自動封鎖程式（Auto Blocker）」與 Message Guard 便屬於此類防禦機制的一環。

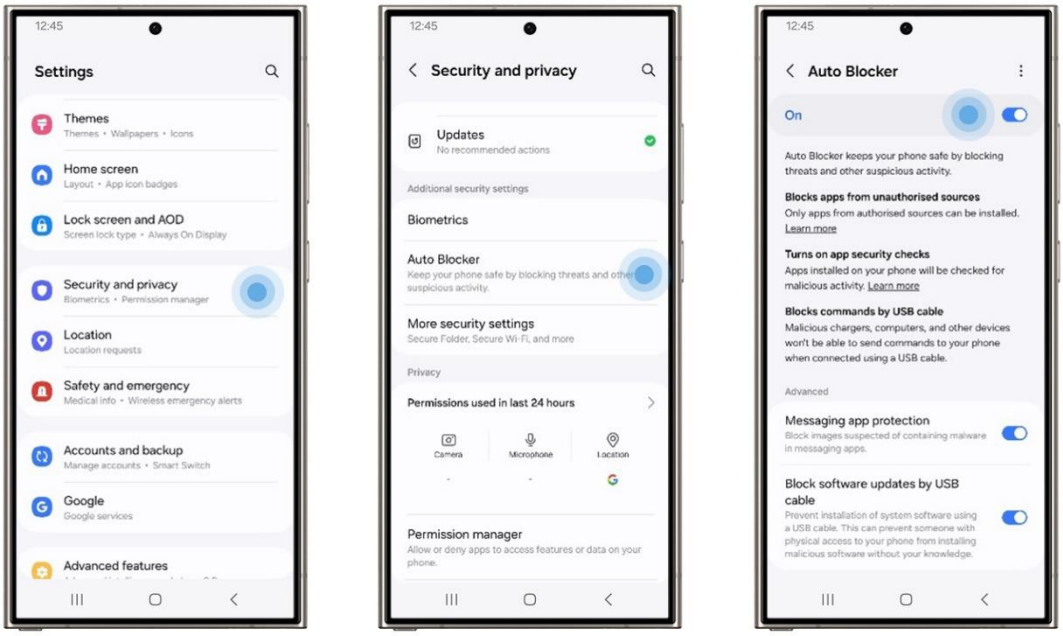
自動封鎖程式（Auto Blocker）

「自動封鎖程式」提供一套附加的安全措施，讓用戶可自行選擇安裝，並全權控制是否要探索 Galaxy 生態圈的自訂功能。「自動封鎖程式」將阻擋裝置安裝未經授權來源的應用程式，藉此保護用戶的 Galaxy 裝置與個人資料。此功能亦會偵測惡意軟體及其他網路安全威脅，並立即對可能造成問題的惡意活動進行封鎖。

「自動封鎖程式」功能之一為防止側載（sideloading），亦即從未經驗證的來源下載應用程式。側載有許多好處，包括可對手機進行進階自訂。若平常沒有進行側載習慣，此功能則能帶給用戶安心保障，並阻止語音釣魚（攻擊者會在電話中誘騙用戶安裝惡意軟體）等社交工程詐騙。

「自動封鎖程式」提供的進階防護措施，能阻擋有害指令進入實體 USB 連接埠，此功能在機場等公共場所內使用插座為手機充電時尤為實用。

只需不到一分鐘，用戶即能以快速簡便的方式開啟「自動封鎖程式」功能：開啟「設定」，前往「安全性與隱私權」，點選「自動封鎖程式」後選擇「開啟」。



▲ 設定 > 安全性與隱私權 > 自動封鎖程式

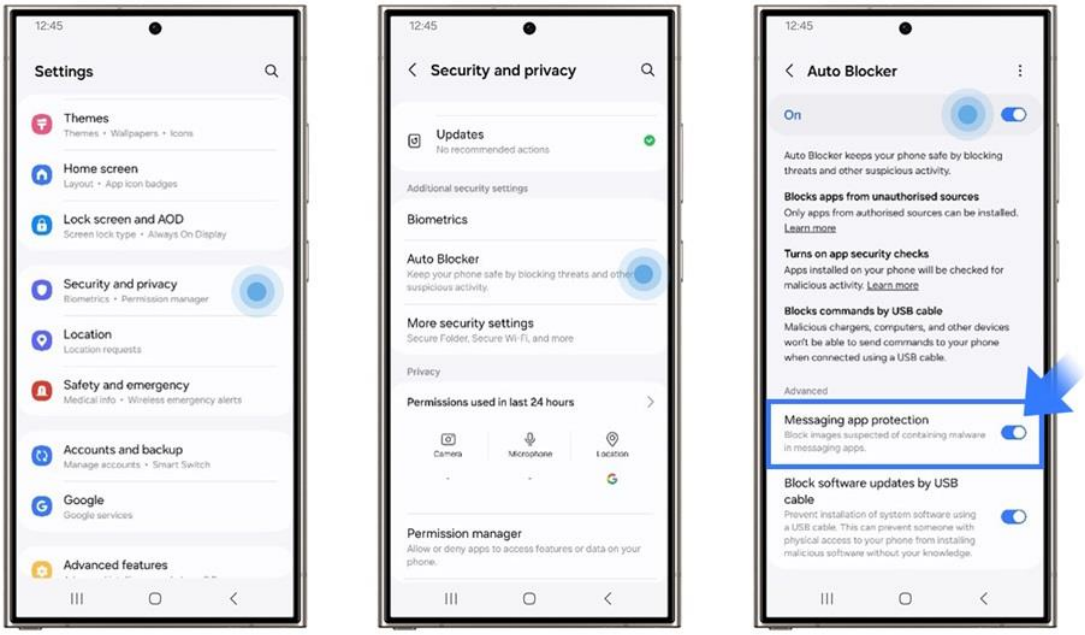
Message Guard

網路安全威脅以多種形式呈現，且每年都變得更加複雜。其中，越來越常見的是利用裝置軟體內的漏洞來進行的零點擊（zero-click attack）攻擊。此攻擊只要在收到圖片時就可能發生，甚至不需要用戶做任何動作。

例如，當手機接收到一個圖檔，僅在用戶口袋裡或床頭櫃上輕微震動一下，即使未觸碰手機或進行任何操作，駭客可能已讀取手機裡的簡訊、瀏覽媒體資料庫，或者複製銀行資料。

三星的 Message Guard 功能透過將檔案封鎖在裝置的獨立空間內，讓隱藏在圖片下的潛在威脅失去效力。當圖片遭到隔離時，Samsung Message Guard 將逐位元檢查檔案，並於受控環境進行處理，確保裝置其餘的部分不受影響。

Message Guard 支援 Google 與三星應用程式、Messenger、Telegram 以及 WhatsApp 等日常使用的多款熱門訊息應用程式。不需仰賴用戶啟用，Message Guard 即隱身於後台，以安靜又有效的方式全年無休於背景運作。

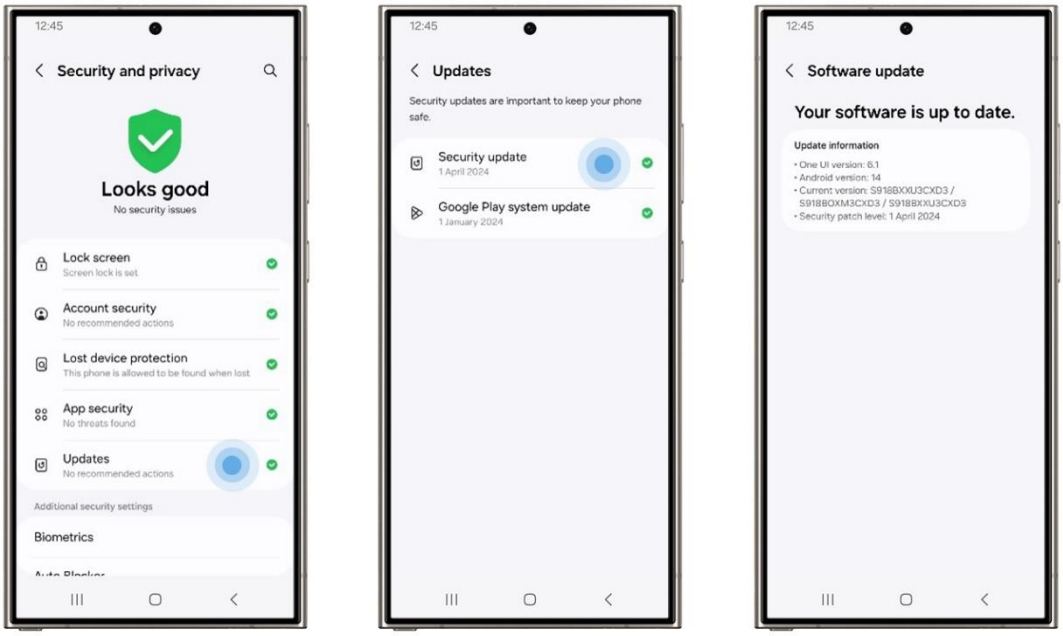


▲ 設定 > 安全性與隱私權 > 自動封鎖程式 > 訊息應用程式防護

網路安全威脅不斷演進且日益普及，三星致力持續守護使用者的資訊安全，唯有全方位的防線，用戶才能保障隱私。無論用戶的生活型態為何，Galaxy 都將堅守崗位 - 守護裝置安全，確保所有大小事皆在掌控之中。

安全更新支援時間延長

擁有強大的安全功能非常重要，但即時更新這些功能亦同樣關鍵，如此才能保護用戶抵禦最新的威脅。因此，自 Galaxy S24 系列(註一)起，三星提供高達七年的安全更新與七代的作業系統升級。此為目前對手機裝置所提供的最長軟體支援時間，進一步延長用戶享有手機安全性與可靠性的體驗。



▲ 設定 > 安全性與隱私權 > 更新 > 安全性更新

註一：Android OS 系統更新、安全更新的支援性與時程，視裝置機型與市場而異。