SAMSUNG

Samsung Message Guard 保護用戶遠離新型與潛藏的威脅

下一個重大的行動資安威脅，可能發生在任何人身上 - 三星已為用戶築起全新防線

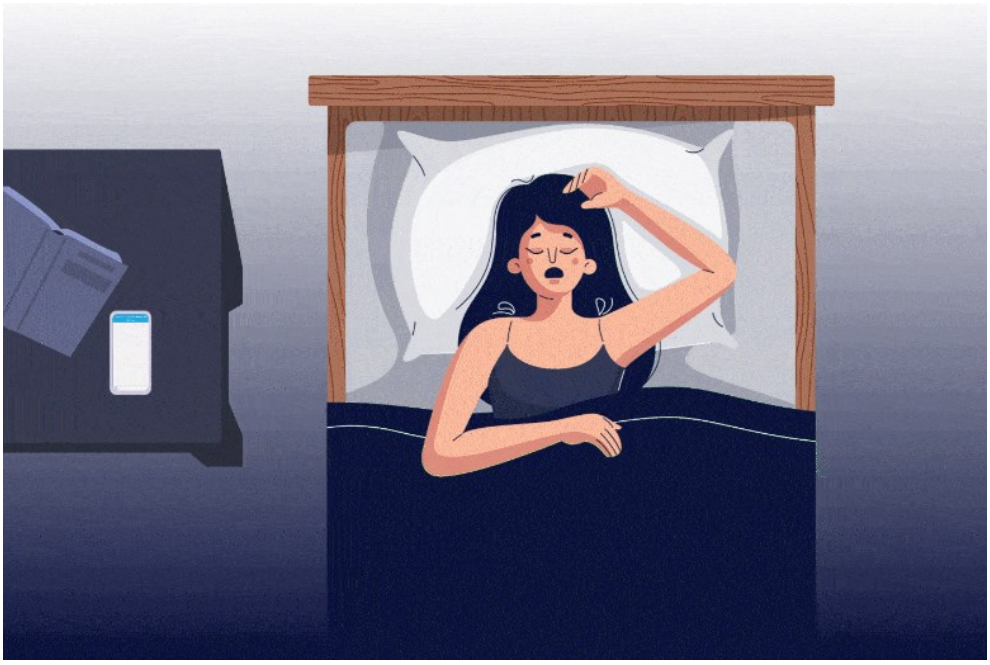
您是否聽聞，僅憑一個接收圖檔的動作，便足以遭到駭客入侵？雖然人人皆知切勿開啟來路不明的連結或附件，但隨著網路犯罪手法不斷推陳出新，這招不再保證萬無一失。

零點擊漏洞是一種新型態的網路攻擊，一旦用戶接收潛藏惡意程式的圖檔，便可能成為駭客的待宰羔羊。

儘管三星 Galaxy 智慧型手機並未傳出此類災情，但三星電子秉持未雨綢繆的理念，持續預測潛藏威脅，並制定先發制人的安全措施 - 例如 Samsung Message Guard。

因應新型態威脅的新防護措施

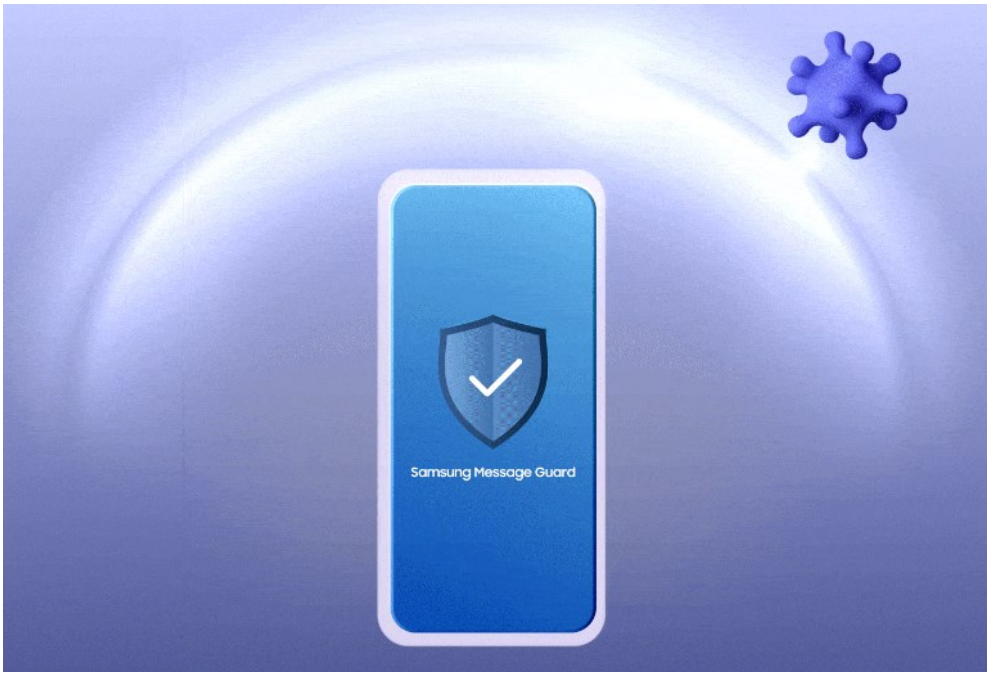
想像下圖中的情景：當手機接收到一個圖檔，僅在口袋裡稍微振動一下；或是手機置於床頭櫃上，可能於用戶睡眠期間短暫亮起。即使用戶未觸碰手機，但駭客可能已經讀取用戶手機裡的簡訊、瀏覽圖庫，並複製用戶的詳細銀行資訊。



鎖定用戶數據的網路犯罪日益猖獗，零點擊漏洞只是最新型態的威脅之一。全球有三分之一的消費者有個資被駭的經驗，為資料外洩的受害者(註一)。資料外洩的現象愈來愈普遍，於 2013 年至 2021 年間的發生率更提升逾兩倍。(註二)

網路威脅不斷演進，而三星的行動資安措施亦更上層樓。三星 Galaxy 智慧型手機以強大的 Samsung Knox 平台作為後盾，為用戶提供全方位的保護措施，避免用戶遭受以影片和音訊格式所發動的攻擊。Samsung

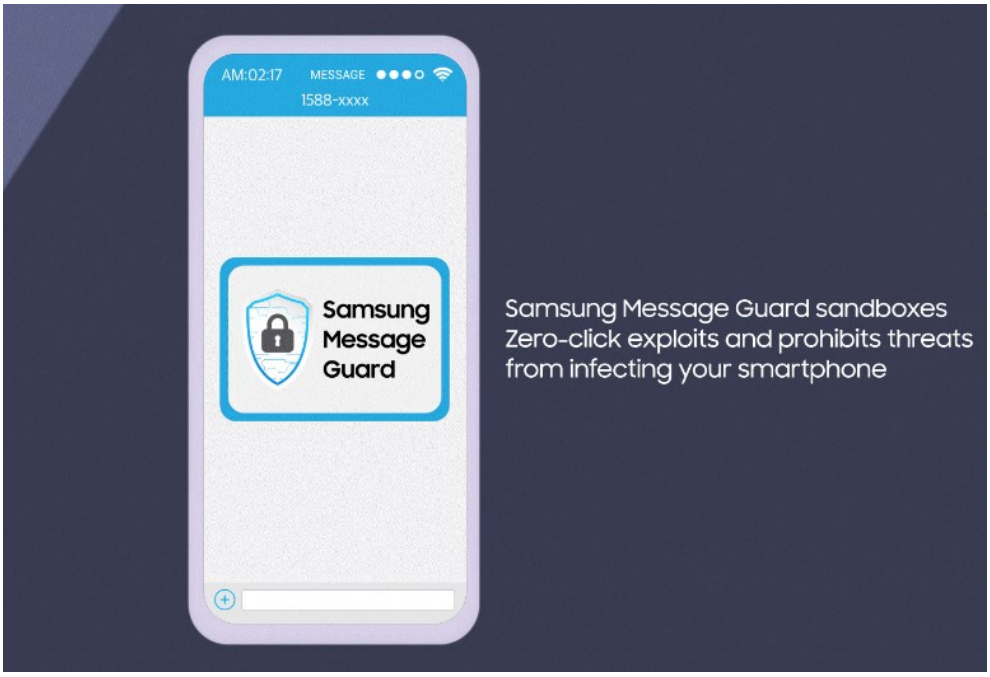
Message Guard 採用先發制人的防範機制，讓用戶遠離以圖檔附件作為掩護的隱形威脅，進一步提升資安保護力[註三]。



該安全解決方案目前應用於 Samsung Messages 與 Messages by Google[註四]。在三星開放式的合作理念下，即將推出軟體更新，使 Samsung Message Guard 得以為用戶提供橫跨第三方通訊程式的防護。

安全的環境

Samsung Message Guard 為一種進化版「沙盒」，或可說是一處虛擬隔離空間。當圖檔傳送至手機時，它會攔截並與裝置的其餘部分相互隔離，此措施可防止惡意程式存取手機檔案、或與其作業系統進行互動。Samsung Message Guard 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。



簡言之，對於隱藏於圖檔中的任何潛在威脅，Samsung Message Guard 會在危害用戶前自動排除。不需仰賴用戶啟動，僅是隱身於後台靜默地運作。因此，以往若置之不理，便可能遭受威脅，現在用戶完全不必動手，即可高枕無憂、無須擔心遭零點擊攻擊。

Samsung Message Guard 是三星最新的前瞻性安全解決方案。此外，在屢獲殊榮的 Samsung Knox 應援下，三星 Galaxy 裝置已於其他領域提供領先業界的資安和隱私保護措施。其提供了橫跨軟硬體各層級的端對端保護，與即時威脅偵測。

上線時間

Samsung Message Guard 為三星 Galaxy S23 旗艦系列的解決方案。今年將陸續於其他 Galaxy 智慧型手機和平板[註五]正式上線。

註一：2022 Thales Consumer Digital Trust Index, https://cpl.thalesgroup.com/data-trust-index

註二：2022 Data Breach Investigations Report, Verizon, https://www.verizon.com/business/resources/reports/dbir/

註三：Samsung Message Guard 之資安防護措施支援下列影像格式：PNG、JPG/JPEG、GIF、ICO、WEBP、BMP、WBMP。

註四：預設通訊軟體應用程式視市場而異。

註五：ONE UI 5.1 或以上版本。