SAMSUNG

【名家觀點】唯有強化資安防護，才能維護隱私權 - 三星與資安社群聯手合作，致力守護用戶安全

▲ Seungwon Shin，(註一) 三星電子副總裁暨行動通訊事業部安全團隊負責人

危險時刻

時值網路犯罪猖獗之際，對於心術不正且具備相關技術知識的人士而言，正是展開攻擊的絕佳時機。

隨著遠距辦公人數攀升，人們對不安全公共 Wi-Fi 的依賴度與日俱增；諸如區塊鏈等新興領域的崛起，讓迷惘的消費者成為詐騙者的待宰羔羊；網路攻擊愈來愈盛行，且出乎意料、令人防不勝防；近期的網路戰模式，更是在物理入侵的數月之前，先對關鍵基礎設施發動一波波數位攻擊。

當人們逐漸將生活重心轉往智慧型手機，潛藏的資安危機正不斷浮現。智慧型手機同時是錢包、大門鑰匙、身份證，一旦遭到入侵，可能造成毀滅性的結果，因此保護裝置安全刻不容緩。讓我們一探三星築起的保護牆，如何嚴密守護裝置安全，讓用戶盡情探索世界，活出自在與從容，不必擔心個資落入宵小手中。

資安的意義與迷思

您可能會因為自己謹慎的安全意識，而覺得一切安好，但人們對於資訊安全普遍存在一些迷思。

例如，您拒絕向應用程式分享個人姓名、電子郵件或習慣，甚至關閉應用程式的追蹤權限。很好，但這並不表示您的個人資料安全無虞。切勿將隱私與安全混為一談，一旦門被踹開，拉上窗簾也徒勞無功。您自認選擇了安全的行動生態圈，猶如一座築有圍牆的花園，但駭客會改變他們的攻擊目標 - 不安全的 Wi-Fi、社交工程詐騙等，無論您使用何種生態圈，威脅無所不在。

您不會開啟可疑的附件。很好，但現在出現了「零點擊」攻擊，不須經使用者互動，依然能破壞設備。Pegasus 是一款間諜軟體，其利用高人氣訊息傳遞系統中的漏洞，讓用戶一接收到訊息，即遭到駭客入侵。當您認為自己的安全意識較高，而陷入自我感覺良好的狀態時，反而正中網路犯罪者的下懷。

網路威脅環伺周遭，若無安全的避風港，著實令人坐立難安 - 這就是 Samsung Knox 的靈感發想來源，其為三星領先業界的國防級安全平台，已獲得全球諸多政府單位認可。三星採用全方位、多層級的防護措施：秉持開放合作理念，整合軟硬體資安防護，並採用即時保護機制。

以合作建構信任

從我與國際刑警組織的合作中，我深刻體悟到團結一心共築安全堡壘、齊力勝過單打獨鬥。開放合作是建構信任的基石，此為 Android 生態圈的一大優勢。任何人皆可存取 Android OS 原始程式碼，集結眾人之力，使其更為茁壯。它能讓科技界的高手相互檢測與挑戰，使寶刀愈磨愈利。

三星對內持續強化系統，對外擁抱開放與合作的夥伴關係，並以此自豪。奠基此理念，三星與 Google 維持長期合作關係，定期召開安全問題會議，相互交流所有的威脅數據。此外，三星亦攜手數百家夥伴，為實現 Android 資安標準化共盡心力。

三星旗下 Galaxy 裝置，亦受益於對三星生態圈瞭若指掌的龐大社群。我們推出「行動安全獎勵計劃」，並與學者、白帽駭客合作，透過定期的安全更新識別和修補潛在漏洞，目前共祭出逾 350 萬美元獎金，號召各路英雄鼎力相助。

三星藉由種種措施，讓安全漏洞無所遁形，甚至及早預測以防範未然；借助眾人的敏銳目光、匯聚專業人士的智慧，提出更完善的解決方案。開放生態圈並未遭致更多漏洞，反而實現更完善、多元化的安全實務作法。

端對端整合措施

這不僅關乎軟體，我們從最細微的處理器開始，嚴密把關每一個元件 - 之所以能辦到這點，正因三星是一家從產品設計到製造，皆由內部包辦的全球一流企業。得益於橫跨三星旗下產品陣容與供應鏈，專為安全而打造的硬體、與外界隔離的軟體，用戶從第一天起，即能獲得滴水不漏的安全保護。因此，我們對旗下裝置的完整性充滿信心：從內部晶片到用戶使用的應用程式，為行動體驗的各個層級，打造端對端的嚴密保護。

隨著世界各地逐步解封，出現諸多有待解決的新風險。因此，三星近期打造更上層樓的 Knox Vault - 結合安全處理器與新型的安全記憶晶片，將諸如 PIN、密碼、生物識別資料、數位憑證、密鑰等最關鍵的資訊，與裝置的其它部分隔開，確保永不落入宵小手中。例如，一旦偵測到裝置出現重大安全風險，Samsung Knox 將鎖住 Samsung Pay 和 Samsung Pass 等敏感服務，使其僅限用戶存取，以維護資料安全性。

時時防護

您是否和我一樣很少關掉手機？但此舉卻讓一些人陷入了麻煩：有些企業誤認為手機開機時的安全驗證，足以保護手機安全。對此，三星即使在啟動階段過後，亦為您的行動體驗打造時刻保護。攻擊者從不休息，我們豈能心存僥倖？

三星致力提供用戶及時保護。開機後，我們的 Real-Time Kernel Protection（RKP）和 Defeat Exploit（DEFEX）技術將繼續運作，並偵測、防止用戶設定的存取權限遭到可疑或未經授權的修改。我們持續監控威脅，甚至建立一支資安事件應變與管理團隊，運用機器學習預測未來的威脅。

雖然很多人年年換新機，但也有一派消費者希望能延長換機週期 - 這就是三星定期發佈安全更新修補漏洞，使裝置自上市起享有五年安全更新的原因。在網路安全快速變遷的環境下，渴望拉長手機使用年限的消費者，應與持有最新機型的用戶，獲得同等級的安全防護。

獲得夢寐以求的隱私，與所需的安全防護

使用者將獲得集所有優勢於一身、世界一流亦兼具安全的行動體驗。三星在開放式合作與產業驗證下，構築一道堅不可摧的保護牆，並結合史上最強悍的硬體規格和軟體防護，滿足用戶對安全的要求。

唯有具備全面性的安全防護，才能為所有人真切打造透明化的隱私，符合個人對輕重緩急的標準。此座安全堡壘，由您作主個人隱私、自由打造所追求的行動體驗，並深知三星守護在側，時時備感安心。

今日的世界比以往更緊密相連，同時伴隨更多風險，但也充滿機會。三星的首要任務，是在用戶探索新體驗的過程中，提供無微不至的保護。Samsung Galaxy 助力用戶活出自在從容 - 獲得夢寐以求的隱私與所需的安全防護。

註一：Seungwon Shin 博士是三星電子副總裁暨行動通訊事業部安全團隊負責人，他執掌三星 Galaxy 生態圈的整體安全創新，包括安全 AP 和 Samsung Knox Vault 開發；亦攜手夥伴與廣大研究社群密切合作，藉由及時防護與威脅預測，監督三星對持續性安全威脅的因應作為。Seungwon Shin 博士亦是國際刑警組織（INTERPOL）暗網小組成員及 FIDO 聯盟韓國工作組主席。在加入三星前，他擔任 KAIST 電氣工程學院副教授，專精暗網研究領域。