嚴阻黑客埋身 築牢手機防線

蘋果(Apple)日前公布現時的 iOS15 系統可能被黑客攻擊，呼籲所有 iPhone 手機及 iPad 用家在 iOS 16 推出前，先更新至 iOS15.6.1。另一邊廂的 Android，較早前有研究報告顯示近半用戶擔心安全問題考慮「轉會」。由於 Android 屬於開放系統，容易下載到未經檢查、包含惡意程式的 App 檔案。為此，Google Play 商店已準備大量新政策，包括打擊錯誤資訊、限制廣告並加強安全性。而不論是 Apple 還是 Android 用戶，也應定期更新作業系統及安裝保安軟件，同時仔細檢查電話及信用卡賬單有否出現可疑收費，如出現以下情況便要加倍留意。

1. 不正常耗電 lag 機

雖然手機電池會隨使用時間而退化，但若手機電池出現異常性的耗電，又或手機出現「lag 機」情況時，有機會是手機中毒徵兆。因為惡意軟體可能挾持了手機，在後台執行任務，導致電力消耗極快或手機運作速度會變得異常地慢。

2. 不明廣告常彈出

若在不明應用程式中不斷出現不會消失的彈出式廣告，千萬不要點擊，否則可能跌入黑客陷阱被盜取個人資料。

3. 機身離奇熨焓焓

在正常情況下，手機不會突然發燙，但某些惡意軟體可能會以內部 CPU 等過度工作，因此導致手機莫名發燙。

4. 附送可疑應用程式

當不慎下載到惡意應用程式時，可能還會夾帶安裝其他應用程式，千萬不要打開，以免加劇中毒。

5. 通話 WiFi 頻斷線

當手機感染了惡意軟體，手機通話和連結 WiFi 等功能也有可能受到影響，因此當手機通話和 WiFi 一直離奇斷線，卻不是信號影響便要小心。

保安加密攻略—iPhone 篇

1. 加強密碼強度

將解鎖密碼更改為混合 6 位數字與英文組合，Face ID 臉部解鎖 / Touch ID 指紋解鎖也要一併開啟。

2. 解鎖畫面權限

在 iPhone 手機尚未解鎖狀態下，不要開太多不必要的權限，透過 iOS「設定」>「Face ID 與密碼」或「Touch ID 與密碼」找到「鎖定時允許取用」，尚未解鎖狀態下，建議將以下權限關掉，能夠有效避免 iPhone 手機遺失造成解鎖畫面權限控制權過大的問題。

- 通知中心
- 控制中心
- USB 配件—防止裝置鎖定超過一小時後，需先解鎖 iPhone 才能允許連線，能防止被破解。

3. 隱藏通知內容

手機重要訊息通知經常會直接顯示在解鎖畫面上，建議將 App 通知內容隱藏起來，防止讓其他人看見傳來的訊息內容。

4. Safari 自動關閉分頁

在設定中的「 Safari 」>「關閉標籤頁」，可以自由設定清除標籤頁期限或選擇手動，避免讓 Safari 愈開愈多，增加安全風險。

5. 防止廣告跟蹤

廣告商會收集使用者的習慣，不想私隱被暴露，可以透過以下步驟關閉：
iOS「設定」>「隱私權」>「Apple 廣告」，開啟「個人化廣告」。

6. 提防釣魚郵件

若收到來自 App Store 的通知取消訂閱郵件便要小心，這些郵件可能是釣魚網站偽裝成官方的訂閱 App 月費郵件通知，模仿蘋果所寄出的風格與排版，誘導用戶直接點擊郵件內的連結，並且輸入 Apple ID 賬戶資料與付款訊息，故在收到通知時，應先確認是否由蘋果官方寄出才點擊。

保安加密攻略—Android 篇

1. 阻擋可疑電話

啟用來電顯示與騷擾/廣告電話功能，提示使用者接到的來電是否來自可疑的騷擾/廣告電話來電者。

2. 加強網站安全

啟用 Chrome 網站安全瀏覽功能，提醒目前瀏覽的網站是否已被判定為不安全的網站，並且可快速協助使用者回到安全瀏覽狀態。

3. 保護 Google 賬戶

遠端攻擊者可能會利用裝置上其他形式的雙重驗證功能，例如透過短訊接收一次性驗證碼和推播通知從事詐騙行為，使用者可使用 Android 內建的安全金鑰，加強 Google 賬戶保護。

4. 管理程式權限

透過系統內建的「管理應用程式權限」，隨時手動撤銷或授與應用程式可存取的隱私權限與相關資料，阻擋惡意程式存取照片或聯繫人等特定類型的資料。

5. 禁止存取位置

除了設定應用程式「隨時都能存取位置資訊」或「禁止存取位置資訊」，也可以手動設定讓應用程式只能在使用應用程式時存取位置資訊。

6. 無痕模式防追蹤

當開啟 Google 地圖中的無痕模式時，系統則不會將 Android 使用者在裝置上的 Google 地圖活動，例如搜尋的地點儲存到 Google 賬戶，也不會使用這些活動為使用者提供個人化的 Google 地圖服務。

7. 啟用 Google Play 安全防護

啟用系統內建的「Google Play 安全防護」機制功能，自動掃描所安裝的應用程式是否安全無虞，如果安裝了可能有害的應用程式，Google Play 安全防護會立即發出警示，並指示使用者如何將這類應用程式從裝置中移除。