



保護個人資料

明智使用智能電話



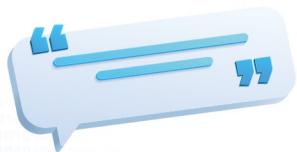
PCPD



HK

PCPD.org.hk

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong



大家現今花更多時間使用智能電話及平板電腦（在此統稱為「智能電話」）。雖然智能電話為我們的生活帶來便利和樂趣，但箇中的個人資料私隱風險實在不容忽視。例如，你的智能電話或會儲存大量敏感資料，如文字訊息、相片、通訊錄，及你的行蹤等。此外，智能電話上的應用程式也可能收集大量有關你的資料。本單張旨在為智能電話用家提供實用建議，在使用智能電話時保護個人資料私隱。







加強 智能電話的保安



**不要對智能電話系統進行
「越獄 (Jailbreak)」或「刷機 (Root)」**

切勿移除智能電話生產商的保安設定（常稱為「越獄」或「刷機」），否則的話，你的智能電話將更易被惡意程式入侵。



安裝防毒軟件

確保防毒軟件正常運作並及時更新軟件。提防免費使用的防毒軟件，因為它們的檔案可能含有惡意程式。



以密碼及/或生物識別啟動鎖屏功能

使用高強度和獨特的密碼可以避免他人在未經授權的情況下查閱你智能電話的內容。同時，請緊記定期更改密碼，亦可以生物識別（例如指紋或面部識別）功能解鎖智能電話。



安裝最新的系統更新

留意並及時更新智能電話的系統，以免你的智能電話遭受最新的安全威脅。



在無需使用時關閉無線傳輸功能

只在有需要使用時才開啟 Wi-Fi、藍芽及近場通訊（NFC），以防止未經授權的追蹤或連接。



避免使用公共充電設施

惡意程式可能會經公眾地方所提供的共用充電器或行動電源散播。如有需要，應使用只供充電而不能傳輸資料的 USB 傳輸線。



啟用「尋找我的裝置」功能

此功能可讓你以遙距方式追蹤智能電話位置、進行鎖機，或在遺失或被盜取電話的情況下刪除儲存於電話內的資料。



在維修或棄置智能電話前刪除資料

將智能電話棄置或送往維修前，利用「回復原廠設定」功能刪除所有資料以防止資料外洩。



保障 儲存於智能電話 內的資料



提防公共Wi-Fi

連接至不可靠的 Wi-Fi 網絡可令你的智能電話和個人資料暴露於未經授權存取的風險。如要進行較高風險的活動，例如使用網上銀行，應使用流動數據。



定期為你的資料進行備份

這可以減低遺失電話或遇到勒索軟件時的影響。如檔案包含敏感資料，應以高強度和獨特的密碼進行加密。



減低使用 應用程式的風險



下載應用程式前細閱私隱政策

了解應用程式會如何收集及使用你的個人資料，並查看它所索取的權限及其他用戶對應用程式的評價。在可行的情況下，選用索取最少必要權限的應用程式。



保護你的應用程式登入帳戶

為每個帳戶設定高強度和獨特的密碼，並定期更改密碼。為進一步加強保安，可以使用多重認證功能（例如透過短訊或電郵收取一次性密碼），以及適時更新應用程式。



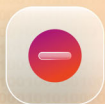
只從官方的應用程式商店下載應用程式

禁止電話安裝從官方商店以外下載的應用程式，因為它們可能藏有惡意程式。



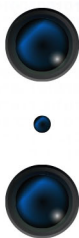
調整應用程式的權限及私隱設定

只容許應用程式存取最少及必要的資料。如非必要，切勿准許應用程式存取你的敏感資料，例如位置、通訊錄、日曆等。



移除不必要的應用程式

定期檢視智能電話上的應用程式，並刪除不再使用或被發現有保安漏洞的應用程式，以防止它們存取或分享你的資料。



PCPD



H K



香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

電話：2827 2827

傳真：2877 7026

地址：香港灣仔皇后大道東248號大新金融中心13樓1303室

電郵：communications@pcpd.org.hk



私隱專員公署網頁
pcpd.org.hk



下載本刊物



本刊物使用署名 4.0 國際 (CC BY 4.0) 的授權條款，只要你註明原創者為香港個人資料私隱專員公署，便可自由分享或修改本刊物。詳情請瀏覽 creativecommons.org/licenses/by/4.0/deed.zh_TW

免責聲明

本刊物所載的資訊和建議只作一般參考用途，並非為法例的應用提供詳盡指引，亦不構成法律或其他專業意見。私隱專員並沒有就本刊物內所載的資訊和建議的準確性或個別目的或使用的適用性作出明示或隱含保證。相關資訊和建議不會影響私隱專員在《個人資料（私隱）條例》下獲賦予的職能及權力。

二零一四年三月（第二修訂版）