

教孩子安全用社群 Apps 爸媽加油讚👍(2)

- 💡 概念篇：智慧型手機開啟孩子的行動社群生活
- 💡 影響篇：孩子隨時隨地打卡，隱私全都露
- 💡 注意篇：行動社群 Apps 也可能暗藏惡意程式
- 💡 法寶篇：不讓孩子捲入行動社群 Apps 危險



【**智慧型手機的普及**】智慧型手機的普及以及行動上網的便利，讓孩子們可以隨時隨地掛在網路上與朋友保持連線，而且手機內的各種社群應用程式 (Apps) 均可共用同一個手機聯絡簿，讓孩子們更方便地悠遊在不同的社群服務中，省去逐一設定朋友清單的麻煩。

【**安裝行動社群 Apps 的代價**】當孩子拿到智慧型手機時，他可能會先下載 LINE、WhatsApp、WeChat 等行動通訊軟體，以便和朋友互傳免費簡訊，然後註冊成為線上音樂的會員準備下載 MP3，並用社群網站如臉書中的某個 App 上傳剛剛自拍的俏皮照片，順便打個卡，期望朋友們看到可以按個讚；接著用手機在自己的部落格上記錄生活點滴，最後再和朋友一起連線玩遊戲 Apps。這些對孩子稀鬆平常的小動作集結起來，卻可能揭露了大量的個人與隱私資料，例如：出生年月日、自己甚至朋友的手機號碼、上傳過的相片或影片、家長的信用卡資料...等。

【**爸媽的提醒，孩子的覺醒**】家長們雖然不見得可以全然掌握各式新興科技與社群服務的發展，但至少可以瞭解孩子們透過手機隨時連結社群網路的風險，並提醒他們在遨遊網路世界與拓展人際關係的同時，應該注意的事項。

孩子在社群網站的「朋友」大半是陌生人

【**數百個社群好友，你都認識嗎**】孩子們在網路上結交的朋友比現實生活更廣泛，除了可能是原本就認識的麻吉、隔壁班不大熟的同學，或朋友的朋友外，還可能是玩線上遊戲所結識的一起攻城的朋友，甚至只是對方部落格上的自我介紹很酷，或照片上是俊男美女，就把對方納入朋友清單。這也是為什麼孩子們動輒有成千上百個網路朋友，但其實他們多半是陌生人。



影響篇 孩子隨時隨地打卡，隱私全都露

【分享愈多，你的隱私就愈少】在社群網站上，只要將某人加為朋友，就表示你所分享的一切，連不熟的網友都看得到。所以，當孩子的網路朋友越多，代表他們可能都知道孩子的個人資料，形同孩子的隱私暴露於高風險中。尤其許多孩子使用行動社群 Apps 分享訊息時，經常會提供過多的個人隱私資料，或是隨時隨地拿著手機拍照並上傳打卡，還要將照片中的其他家人或朋友逐一加上 tag (標籤)，把大家的行蹤即時在網路上「轉播」。分享生活點滴並獲得朋友回饋固然有趣，但是也可能因此遭到有心人士的惡意追蹤，造成自己或家人的傷害。

歹徒看臉書打卡記錄綁架少年

臺中一名家境富裕的少年經常在臉書上打卡，歹徒因此掌握少年的行蹤與作息，於綁架少年後向家屬勒贖 500 萬元。【摘自 華視 2013.03.19】

陌生人加孩子為社群 Apps 好友，拐騙、援交樣樣來

【陌生人可輕易將孩子加為好友】大多數的行動社群 Apps 都提供便利的搜尋與加入好友功能，以國內使用者最多的 LINE 為例，只要智慧型手機的通訊錄有對方的電話號碼，LINE 就會自動將他們加為好友。因此，若陌生人取得孩子的手機號碼，而孩子也有安裝 LINE，如果沒有關閉「允許被加入好友」功能，陌生人便可輕易地將孩子加為好友，任意傳送訊息，甚至是色情簡訊或圖片。

【惡意人士可能藉此騷擾】國內外已發生歹徒利用行動社群 Apps 進行騷擾、誘拐以及援交的社會案件，受害者包括未成年孩童。部分國家如日本的警政機關因此開始針對青少年與孩童進行 LINE 的安全使用宣導。

歹徒利用 LINE 誘拐 13 名未成年少女賣淫

在三重開設傳播公司的游姓男子以 LINE 聊天軟體尋找輟學少女簽約賣淫，並涉嫌性侵 13 名未成年少女。警方查獲後，以妨害性自主、妨害風化，及違反兒少法等罪嫌將歹徒移送法辦。【摘自 中時電子報 2013.03.14】

注意篇 行動社群 Apps 也可能暗藏惡意程式

【智慧型手機也可能中毒】智慧型手機就如同一部迷你電腦，有處理器、記憶體與儲存空間，可以安裝各種 Apps 軟體與上網玩遊戲、瀏覽影音等，也因此，智慧型手機和電腦一樣，都會遭受惡意程式的威脅。這些惡意程式可能會竊取手機中的個人資料，或偷偷地發送垃圾郵件、詐騙簡訊，還可能讓手機的記憶卡資料被破壞摧毀。

【手機安全威脅持續升高】針對智慧型手機的安全威脅，各大資安廠商的研究結果一致指出，目前已有超過百萬個手機 Apps 含有惡意程式和漏洞，而且惡意 Apps 的數量正逐年增加，且預估未來也將持續增長。

【熱門 Apps 山寨版藏危機】在各種手機 Apps 中，熱門的遊戲與社群 Apps 最容易成為惡意開發商和網路犯罪分子的目標。過去曾出現數個知名 Apps 的惡意山寨版，有些是安裝後，程式會自動地每隔 15 分鐘將手機用戶的位置資訊傳送到特定的伺服器，造成民眾在不知情下被定位追蹤；有些則是啟動後，程式會自動傳送付費簡訊，導致手機用戶的傳輸費莫名其妙地暴增。

Candy Crush 通關密技 App 侵犯個人隱私

頗受歡迎的手機遊戲 App 炸糖果(Candy Crush)日前出現號稱提供玩家通關密技的 App，民眾一旦安裝後，除了會持續收到廣告通知外，還會導致位置行蹤、SIM 卡號碼等隱私與重要資訊的外洩。【摘自 賽門鐵克 2013.07.27】



1. 教導孩子絕不答應或回應陌生人傳來的見面邀約。
2. 教導孩子當收到下列危險訊息時，一定要馬上封鎖對方，並告訴長輩自己收到這樣的訊息：
 - 提出具有性暗示的問題，例如：詢問有沒有性經驗；
 - 要求寄照片；
 - 詢問性別、年齡、就讀學校，或是住在哪裡；
 - 詢問外貌長得像哪位藝人、體重、身高、胸圍等身體特徵；
 - 詢問家裡電話號碼、地址、個人 E-mail 等聯絡方式；
 - 還不認識就稱讚「好可愛」，或發送「我好像喜歡上你了」、「你應該是我喜歡的類型」等訊息；
 - 不斷試圖邀約見面；
 - 強調「我可以買 OO 給你唷！」，試圖表現自己很有錢，或是主動提出要給零用錢；
 - 自稱從事演藝事業相關工作，詢問「想不想當模特兒？」、或是「要不要我介紹哪位藝人給你認識」。
3. 教導孩子使用行動社群的「封鎖朋友」或「取消朋友」等功能(以 LINE 為例，其「封鎖」功能操作步驟請至官網查詢「封鎖」)。
4. 教導孩子不可和陌生人交換自己行動社群 Apps 的帳號或暱稱等個人資訊，也不要再在網路上公開自己的帳號或暱稱。
5. 有些行動社群 Apps 只允許授權對象把自己加為好友的功能。為了避免被陌生人加為好友，應協助孩子進行相關的設定(以 LINE 為例，可關閉 LINE 的「允許被加入好友」與「公開 ID」功能，操作步驟請至官網查詢「允許被加入好友」、「公開 ID」)。
6. 若仍然遇到問題，或收到內容奇怪的訊息時，讓孩子知道還可以向誰求助，例如：家長、學校老師、學校輔導室...等。

教孩子安全用社群 Apps

爸媽加油讚  (2)

出版者	教育部
發行者	蔣偉寧 教育部部長
召集人	梁理旋 財團法人中華民國國家資訊基本建設產業發展協進會協理
指導委員	楊鎮華 教育部資訊及科技教育司司長 劉文惠 教育部資訊及科技教育司副司長 林燕珍 教育部資訊及科技教育司高級分析師 許雅芬 教育部資訊及科技教育司數位學習科程式設計師 劉玉珍 教育部資訊及科技教育司數位學習科程式設計師
審查委員	林杏子 國立高雄大學資訊管理學系教授
撰稿人員	梁理旋 財團法人中華民國國家資訊基本建設產業發展協進會協理
承辦單位	財團法人中華民國國家資訊基本建設產業發展協進會
出版日期	102 年 11 月



本著作採用創用 CC「姓名標示、非商業性、相同方式分享」授權條款釋出。

創用 CC 內容請見：

http://creativecommons.org/licenses/by-nc-sa/3.0/tw/deed.zh_TW

※ 此手冊內容係對特定議題所提供之學習教材，僅供各界參考，非本部相關政策。