



智慧型手機安全管理



本簡報內容著作權為NII產業發展協進會所有

•



大綱

1. 威脅案例
2. 安全管理

•



臺灣民眾愛用手機上網

最黏手機 大國家排行榜

國家	平均使用手機 上網時數(分鐘/天)	國家	平均使用手機 上網時數(分鐘/天)
1 台灣	197	7 香港	162
2 印尼	181	印度	151
3 菲律賓	174	9 美國	144
4 中國	170	10 南韓	144
5 越南	168	世界均值 142	
6 泰國	167		

資料來源/MillwardBrown & Yahoo
Survey of AdReaction2014
製表/蕭韻純

聯合報

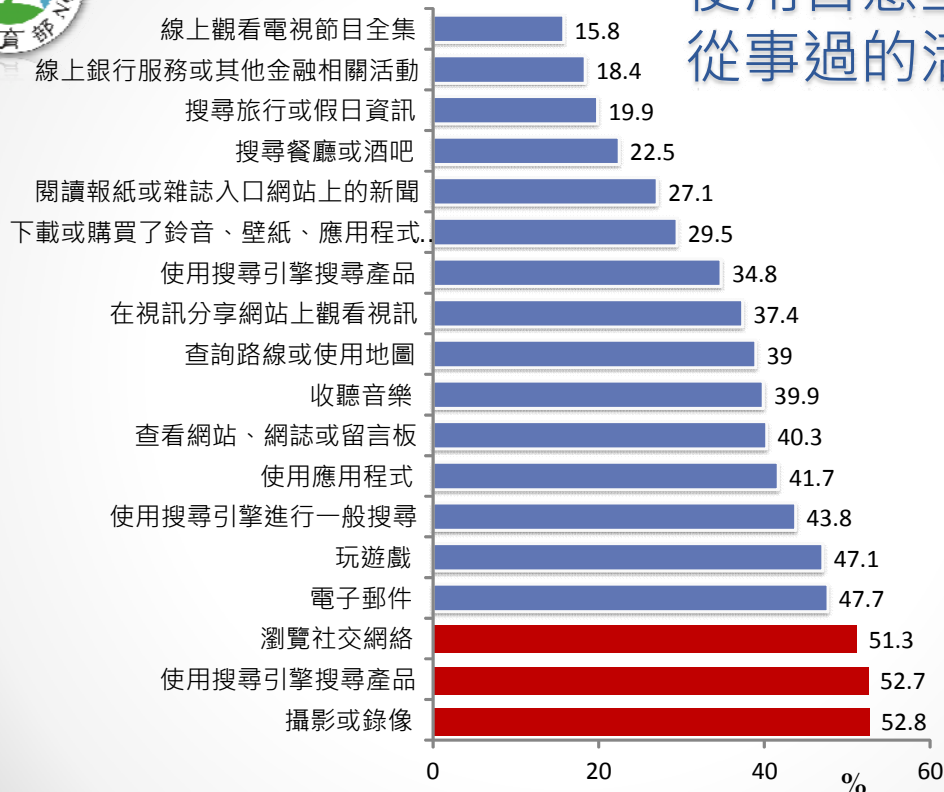
圖/聯合報

資料來源：聯合報

● 7



臺灣民眾最近 7 天內 使用智慧型手機 從事過的活動



資料來源：Our Mobile Planet (Google) · 製圖：NII產業發展協進會

● 8



威脅與案例

• • •

• 9



智慧型手機十大安全風險

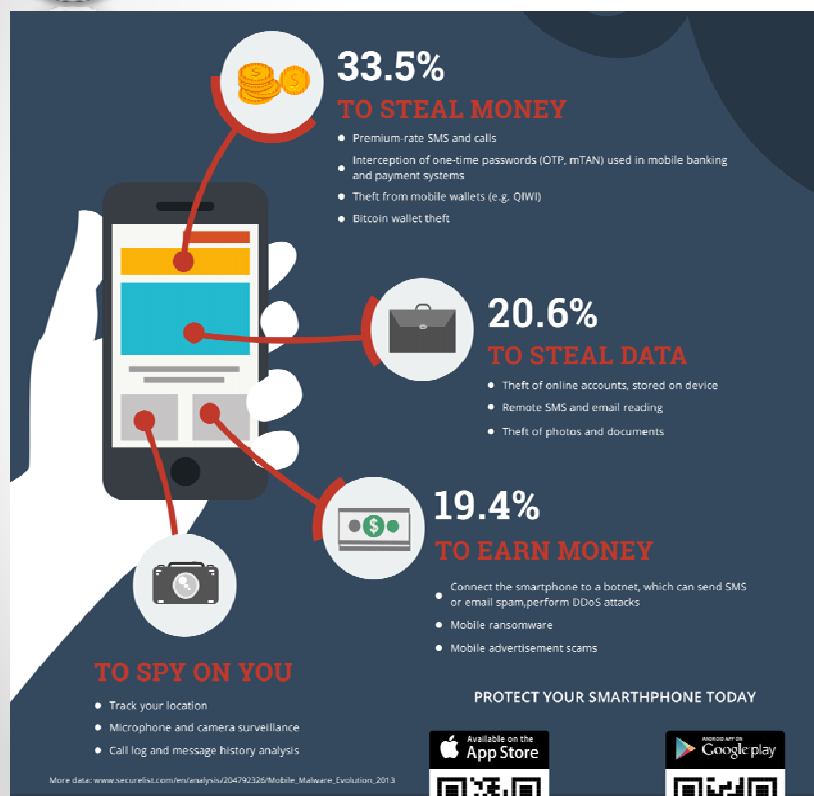
#	安全風險	威脅度	說明
1	因手機遺失或被竊的個資外洩	高	手機被竊或遺失後，因手機內建硬碟或記憶卡內所存放資料沒有做任何加密保護，使得重要個人資料外洩。
2	無意的資料外洩	高	使用者因不清楚手機各項App的功能，部分App會蒐集與利用使用者的各項資訊，例如GPS功能開啟後可追蹤使用者的所在位置。
3	報廢手機未清除機內資料	高	報廢手機前，未妥適地清除機內資料，使得資料外洩。
4	手機釣魚	中	利用山寨版App或隱含釣魚網站超連結的簡訊等方式，誘騙使用者輸入其個人相關資料。
5	間諜程式	中	被植入間諜程式的手機可允許駭客偷偷地存取手機內的個人資料
6	Network Spoofing	中	攻擊者以假的Wi-Fi上網存取點誘拐使用者連上網，隨後再攔截（或篡改）使用者在網路上傳輸的內容。
7	監控	中	透過間諜程式，針對特定使用者的手機進行監控與追蹤。
8	自動撥號或傳訊	中	攻擊者可在使用者不知情的狀況下自動撥打手機號碼（付費電話或傳加值型簡訊（較一般簡訊費用高）。
9	金融資料竊取	中	手機感染特別針對竊取金融資料（如信用卡號碼、網路銀行帳號與密碼）的惡意程式。
10	網路塞車	低	當手機保持在線上狀態時，某些APP會不斷嘗試下載或更新資訊導致網路資源耗盡。

資料來源：[European Union Agency for Network and Information Security](http://ec.europa.eu/networks/index_en.htm)

• 10



駭客想一窺究竟手機的原因



圖案來源：Kaspersky Lab
<http://blog.kaspersky.com/hackers-smartphone-infographic/>

● 11



常見威脅 1. 來自傳訊服務的惡意連結詐騙

● ● ●



假官網，真詐騙

山寨版LINE假官網騙走帳密

若利用雅虎搜尋關鍵字「Line」結果會出現 LINE 關鍵字廣告，該廣告顯示的 LINE 官網的網址為 <http://line.me/zh-hant/>，但實際上該網址會將使用者帶到假官網，網址為 <http://line.pm/zh-hant/>。

一進入該釣魚網站，會先要求使用者登入 LINE，一旦登入，自己的 LINE 帳號和密碼即被竊取。

【摘自 電腦王阿達的3C胡言亂語 2014.05.11】



圖片來源：電腦王阿達的3C胡言亂語 · <http://www.kocpc.com.tw/archives/5083>

● 13



圖片來源：電腦王阿達的3C胡言亂語 · <http://www.kocpc.com.tw/archives/5083>

● 14



圖片來源：[電腦王阿達的3C胡言亂語](http://www.kocpc.com.tw/archives/5083) · <http://www.kocpc.com.tw/archives/5083>

● 15



送免費 LINE 貼圖？

FB 送免費LINE貼圖？

今年初曾流行一則「FB 臉書免費贈送 LINE 貼圖」的訊息，該訊息透過 LINE 傳送，內容提到只要點選訊息內網址，並轉發20人後就能領取免費貼圖。

經查證發現，原來該訊息會將使用者帶到一個釣魚頁面，為的是要騙使用者輸入臉書帳號與密碼。

【摘自 ifans 3C | 林小旭 2014.03.04】



圖片來源：ifans 3C | 林小旭 · <http://ifans.pixnet.net/blog/post/174122292#comment-33728802>

● 16



- 圖片來源：ifans 3C | 林小旭 · <http://ifans.pixnet.net/blog/post/174122292#comment-33728802> ● 17



訴訟通知其實是惡意程式

運將誤點收訴訟單簡訊連結遭詐騙

一名計程車司機接到手機簡訊，內容為「台北地院民事賠償訴訟通知單」並附連結網址，點下網址後進入空白網頁，而實際已下載惡意程式。

隔月司機收到手機帳單才發現，多了一筆購買遊戲點數的小額付款交易\$1,000，這時才驚覺遭到詐騙。

【摘自 自由時報 2014.06.22】



- 圖片來源：內政部警政署 <http://www.spfh.gov.tw> ● 18



手機/LINE詐騙簡訊一覽表

#	來自朋友
1	「0809.....，用手機打給我一下，新辦的,幫忙測試一下」
2	「○○○這是你那晚沒來的照片，我被整慘了...」
3	「我的手機送修，麻煩替我收個簡訊好嗎？」
4	「拜託收幾封購物簡訊，我有急用！」
5	「看看那些年我們合拍的照片是多麼年輕」
6	「○○○我在墾丁拍的照片，你覺得哪張最好看。」
7	「○○○這是上次聚會的照片，你好好笑」
8	「是○○○麼？老同學來看我現在的照片能想起來我是誰嗎..」
9	「○○○看著這些照片，好懷念以前的日子！」
10	「○○○這是上次同學聚會的照片，大家都有來」
11	「○○○我們中秋烤肉的照片,好多人喔」
12	「○○○朋友家狗狗參加人氣比拼，幫忙讚一下」
13	「○○○朋友參加攝影比賽幫忙投票」



● 資料及圖片來源：雲端運算與網路安全趨勢部落格 · <http://blog.trendmicro.com.tw/?p=6279>

● 19



手機/LINE詐騙簡訊一覽表

#	來自政府單位
1	【新北市政府警察局通知單】您涉嫌的案件處理結果通知單
2	「○○○女士您有交通罰單逾期未繳...」
3	你的民事賠償訴訟通知單【台北地院】

#	來自網購
1	「○○○先生,你的露天商品已經送達門市，寄件代碼: http://goo.gl/uq**** 」
2	「您的快遞簽收通知單，收件電子憑證: ○○○ 網址」

#	來自電信公司
1	「○○○女士,您的電信本月應繳費賬單,查詢電子帳單...」
2	「尊敬的客戶您好，您的手機正在申請6800元的網路支付，如非本人操作請加載電子憑證確認取消...」

#	時事
1	「您正在申請網上支付103年○月電費共計480元，若非本人操作，請查看電子憑證進行取消」
2	fb 免費送貼圖,把此消息轉發十五個LINE好友,可以免費領取價值一百的貼圖表情,領取地址...」
3	「學運受傷學生急需醫藥費！」



最新簡訊詐騙：
露天商品送達通知

● 資料及圖片來源：雲端運算與網路安全趨勢部落格 · <http://blog.trendmicro.com.tw/?p=6279>

● 20



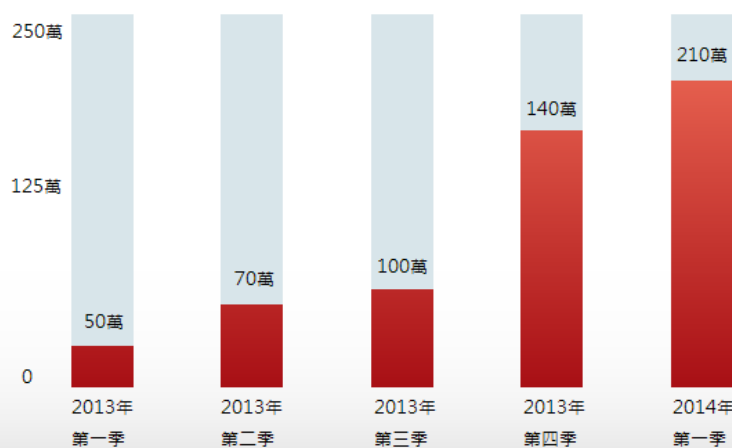
常見威脅 2. 惡意手機應用程式 (Apps)

...



高風險 Apps 數量突破二百萬

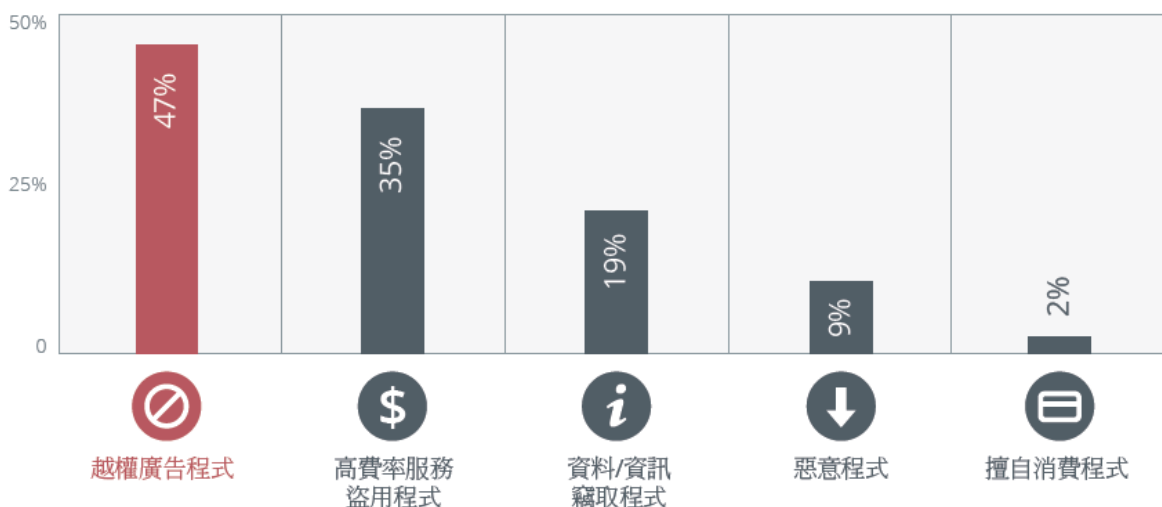
Android 威脅數量成長趨勢 (2013 年第一季至 2014 年第一季)





越權廣告登 Android Apps威脅首位

Android 領先威脅類型分布比例



- ✓ 越權廣告程式會不斷顯示廣告，甚至可能暗中蒐集個人資訊。
- ✓ 高費率服務盜用程式會暗中幫受害者註冊特別昂貴的服務。

圖案來源：TrendLabs 2014 年第一季資訊安全總評

● 23



侵犯隱私的惡意 Apps 逐年成長

2012

2013

ANDROID MALWARE ALMOST TRIPLED
from 2012 to 2013, with more collection of
handset information, premium SMS scams,
fraud, downloaders, and installers



OF THE MOST PRIVACY-THREATENING APPS
also contain malware

35%最具隱私威脅的Apps
內含惡意程式。

2013年Android 惡意App
的數量是前一年度的三倍。



OF APPS TRACK YOU
they know: when you use Wi-Fi and data
networks, when you turn on your device, and
your current and last location

82%的App會追蹤你的個資。

圖案來源：McAfee Mobile Security Report (February 2014)

● 24



案例

四款影音Apps暗藏木馬程式

香港媒體委託資安公司針對市場上數款 Apps 進行測試發現，包括App PPTV、PPS 影音、優酷視頻、風行視頻等Apps，均含有木馬程式。

此款名為Android.Spy.origin.83 的木馬程式，會偷窺手機內存放的照片，進行偷拍及竊聽。

【摘自中時電子報，2014.08.12】

2014 FIFA 開踢，惡意 App 暴增

2014年的FIFA世界盃足球賽才開踢沒幾天，資安公司已偵測到超過375種惡意Apps，這些惡意Apps多潛伏在未經授權或第三方App下載商店，等待使用者下載。

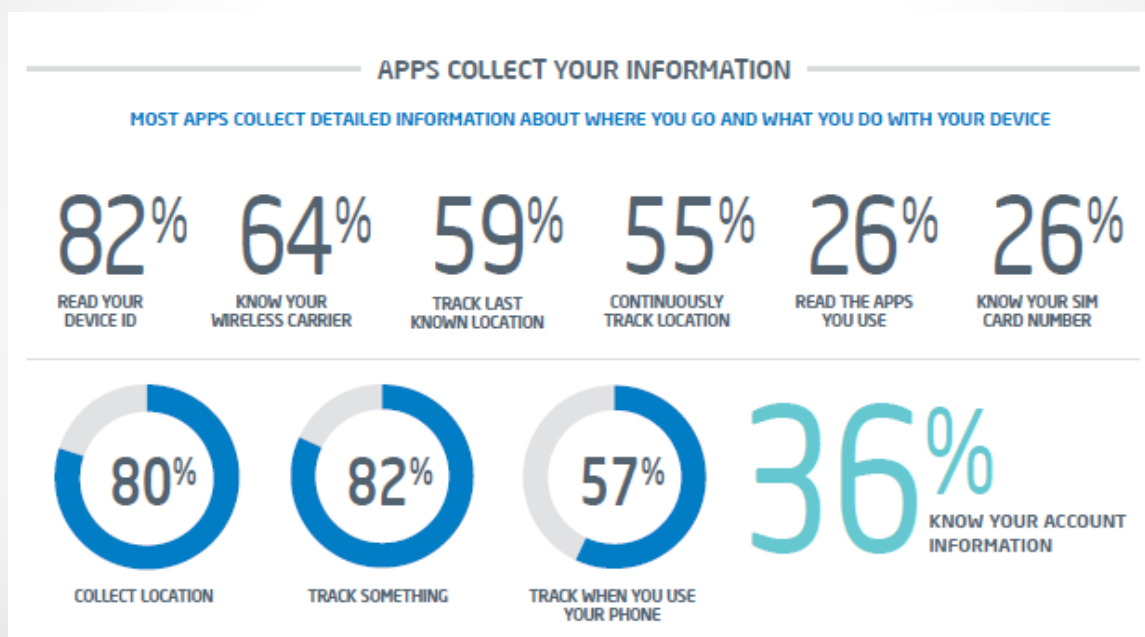
惡意的FIFA Apps 會私下過濾簡訊、竊取資料、發送簡訊、安裝新惡意軟體、或誤導使用者付費消費等。

【摘自趨勢科技，2014.06.16】

● 25



Apps 會蒐集那些資訊？



圖案來源：McAfee Mobile Security Report (February 2014)

● 26



常見的可疑 Apps 類型

類型	說明
山寨版	受歡迎的 Apps，特別是遊戲或付費的 Apps，會出現免費的山寨版；伴隨來的廣告可能會提高收到垃圾訊息或揭露個資的風險。
色情類	色情類的 Apps 服務通常會刻意將結帳金額搞得很不清楚，讓使用者不小心付了一大筆錢。
假防毒	假防毒 Apps 只提供相當低程度的保護，卻收取高額的費用；惡劣的防毒 Apps 甚至會宣稱手機已中毒，要求付費才能解除問題。
賺錢類	號稱只要看廣告、或者提供存取手機簡訊服務授權同意，就可以賺錢的 Apps，此類型的 APPs，可能違反使用者與電信公司間的服務協議。



● 資料來源：Lookout Inc. (February 2014)

● 27



Virus Shield

Deviant Solutions - April 2, 2014
Social

\$3.99 Buy

Add to Wishlist

★★★★★ (1,288)

8+ 175

在 Google Play 的售價 \$3.99

上線一週下載人次超過萬人

thanks a lot! It is updated and running great! you fixed it!

Reviews

4.5

★★★★★

584 total

5 425

4 5

3 2

2 4

1 3

★★★★★

★★★★★

★★★★★

★★★★★

★★★★★

★★★★★

★★★★★

★★★★★

★★★★★

★★★★★

★★★★★

★★★★★

★★★★★

★★★★★

★★★★★

★★★★★

★★★★★

★★★★★

★★★★★

★★★★★

★★★★★

★★★★★

★★★★★

★★★★★

★★★★★

★★★★★

★★★★★

★★★★★

★★★★★

★★★★★

最高曾獲得 4.7 顆星評價

When I downloaded this app my phones seem to run faster

works in background and doesn't harm my battery



唯一的機能就是將 X 變成 ✓

Google 已將該 App 下架

根據媒體報導，Google 已通知下載 Virus Shield 用戶全額退款，並提供價值 5 美元的 Google Play 點數，讓使用者可用於購買 App、音樂、書籍等內容。



賺錢 Apps 的賺錢方式



號稱不必做任何事情（除了下載與安裝 App），就可以賺錢。

- 帳戶餘額達 \$5.00 時，即可領錢
- 第一次登入馬上送 \$1.00 紅利
- 用戶未使用的簡訊數量，由 App 開發商買下，每則 \$0.001
- 每個月最高可賺進 \$30.00
- 該 App 會以用戶手機傳遞所賣出的簡訊

App 開發商號稱絕對不會發垃圾信，其客戶都是銀行、飯店、航空公司等，且簡訊內容以確認碼、班機資訊、飯店預訂確認函為主。

因為簡訊寄送由該 App 於背景中執行，用戶不知道自己傳送了哪些訊息出去。

● 參考資料：Lookout Inc. (February 2014) / Google Play

● 29



為何手機容易被拿來詐騙？

- 手機使用者對各式手機服務或軟體應用的安全選擇較不熟悉，且通常也很自然地就在手機中輸入個人資料。
- 智慧型手機螢幕大小有限，不容易讓使用者從中判斷合法與偽造網站間的差異（且許多網站都設置手機版頁面，使得判斷難度增加）。
- 民眾下載 Apps 的習慣通常不包括進一步瞭解該應用程式開發者是誰，也讓駭客有機可乘。

●

● 30



常見威脅 3. 無意間洩漏個人資料

...

● 31



假民意調查，真個資蒐集

駭客針對臺灣走上街頭者蒐集個資

自5月份開始，陸陸續續許多臺灣民眾的 iPhone 收到了 iMessage 民調簡訊，共有「服貿是過還是死」、「核四廢存之爭」、及「下一次你是否會走上街頭？」等三個題目。

因投票時並不需要輸入姓名或手機號碼，讓人以為是「匿名投票」，而實際上每個人收到的投票網址不同，對於誰投了甚麼票，留下哪些意見，都有完整紀錄。

【摘自 阿瑪外傳 2014.05.14】

SOS 核四廢存，民生大計！
SOS 封存只是 1 時，或停或
建總要決定！不空喊民主大
義 ✕ 不觀望政客角力 ✕ 參
與投票，表達真實意願
[http://vote.tw.am/?
d=62qFZ,eO](http://vote.tw.am/?d=62qFZ,eO)
！「民意」不能輕易被利用
！大嘴鄭重公告，上一輪投
票中，52.4%的民眾支持通
過服貿協議。✓ 感謝表明態
度的你！👍

導航			
首頁			
用戶反饋			
投票記錄			
無號碼投票記錄			

ip	參與投票	留言
109	核四廢存之爭	台灣地質不適合在興建核四，改用太陽能來取代核四。
153	核四廢存之爭	興建核四，害子害孫。
38	核四廢存之爭	經濟要死了
42	核四廢存之爭	核四已建許久現今再來說議題有這必要嗎！台灣不能再虛耗時光。
184	核四廢存之爭	或許核電是最快最有利的資源，但它也是消耗我們最快的。希望大家不要只看眼前利益，眼光放遠一點，想想後代的未來好嗎？
105	核四廢存之爭	安全與民生優先考慮
47	核四廢存之爭	電夠用嗎？火力發電廠不會污染？每日燃燒多少噸的煤能不排除二氧化碳嗎？有電當思無電之苦
	核四廢	建設無核家園，保護台灣

choicevote_item_kid	date	iphone
137.84	2014-04-30 21:29:35	8869884
158.8	2014-04-30 21:29:43	8869820
04.125.1750	2014-04-30 21:30:24	8869153
9.142.239	2014-04-30 21:30:30	8869869
114.178	2014-04-30 21:30:43	8869117
22.248	2014-04-30 21:31:15	8869379
50.131.1960	2014-04-30 21:32:26	8869321
07.146.2531	2014-04-30 21:33:15	8869159
43.246.1771	2014-04-30 21:33:49	8869300
76.6.31	2014-04-30 21:34:00	8869895
201.212	2014-04-30 21:34:45	8869119
04.84.148	2014-04-30 21:35:20	8869876
10.149.2190	2014-04-30 21:36:19	8869891
2.221.227	2014-04-30 21:37:15	8869112
159.10	2014-04-30 21:37:43	8869323
5.201.127	2014-04-30 21:37:56	8869219
246.193	2014-04-30 21:38:49	8869212
74.9.235	2014-04-30 21:39:01	8869320
68.97.74	2014-04-30 21:39:06	8869866

● 圖案來源：阿瑪外傳 <http://armorize-cht.blogspot.tw/2014/05/apple.imessage.apr.campaign.html> ● 33



自願與非自願洩漏個資

入口網站加密相簿，手機瀏覽不設防

國內知名入口網站的網路相簿功能，被網友發現其放在上鎖加密相簿內的照片，若是透過智慧型手機以「手機版」網頁瀏覽該相簿時，可以不需密碼就看得內容。

入口網站回應該問題是由於內部作業時，手機版本沒同步更新所導致。在媒體揭露該消息後，廠商已修正調整手機版相簿的問題。

【摘自 蘋果日報 2014.02.10】

打卡炫耀詐騙百萬鈔票遭警逮補

板橋一名老先生因兒子出差被詐騙集團盯上，稱兒子已被綁架，要求1百萬現金贖款。詐騙集團的車手拿到百萬現金後，拍下兩疊厚厚鈔票的照片上傳到臉書並打卡，警方鎖定其打卡位置據以逮人。

【摘自 TVBS 2014.08.08】



常見威脅 4. QR Code

...



臺灣首例QR Code駭客攻擊

臺灣首見的QR Code駭客攻擊案發生在今年2月份，在人潮洶湧的某個台北捷運站內所刊登的一則大型旅遊廣告看板中，印有一組 QR code，若用 Android 手機掃描，竟然連往俄羅斯色情網站、並且下載可疑的 App 程式。

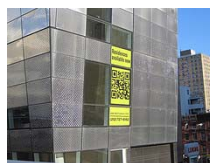
【摘自數位時代 2014.03.13】

事件學習

掃描 QR Code 下載 Apps 為常見使用情境，此手段容易讓消費者上當。

駭客只對手機用戶做攻擊，網站管理人員通常利用桌機檢查網頁，不易發現手機版網頁出問題。

駭客在技術上可以做到把銀行、網購、航空公司或各類 QR Code 轉址到假 App 下載。



圖片4



圖片5



常見風險 5. 智慧型手機遭竊/遺失/販售

...

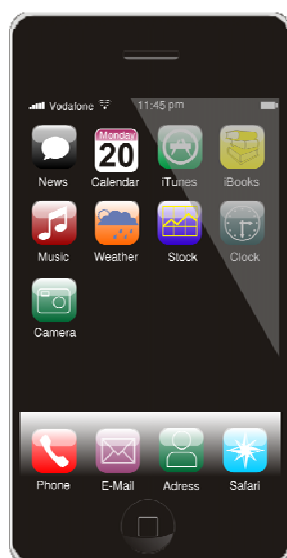
● 37



手機掉了很嚴重嗎?

包含大量有價值的資訊

- 通訊錄個人資料
- 各式社群網路服務帳號
- 電子郵件帳號
- 信用卡號碼
- 各式網路服務密碼.....



若手機用於公司用途，可能還包含

- 客戶資料
- 企業電子郵件訊息
- 公司內部文件.....

遺失或遭竊的智慧型手機內的資料若無妥善防護機制
(例如加密)，有心人士便有機可乘！！

● 38



案例

手機遺落桌上，後方男子隨即撿走

臺中市一名男子在買彩券時，因填寫號碼將手機放在彩券行門口的桌子上，才走幾步路立刻回頭找手機沒想到已遺失。

調閱監視器畫面後才發現，後方另一名男子看到手機後隨即拿走。遺失手機的男子表示，自己的舊手機其實價格不高，但裡面儲存不少照片及資料，丟了很麻煩。

【摘自自由時報 2014.08.06】

小米機遺落計程車，網銀被盜千元

大陸一名在軟體公司上班的青年搭乘計程車，不慎將剛買2個月的小米機遺落在車上，隨後其綁定手機的網路銀行服務被盜刷了1千元（人民幣），微博和WeChat帳號也被盜用。

更讓他懊悔的是，其手機內存放著大量的客戶與公司資料，遺失後可能造成更大的損失。

【摘自合肥晚報 2014.07.30】



題外話

遺失預付卡被盜用，男子被起訴

一名男子手機遺失後，因易付卡門號餘額所剩不多，因此未將門號掛失，結果被詐騙集團拾獲後用於詐取他人錢財。檢察官以男子提供門號給詐騙集團使用，將他視為共犯起訴。所幸法官認為，被告遺失的門號卡內還有餘額，如要販售門號卡，應將餘額用完才交付卡片，與常理不符，判他無罪。

【摘自自由時報 2014.07.27】

謊稱幫忙保管手機，法官判竊盜

一名外籍英文老師在臺北市的酒吧消費，趁老闆不注意時偷走吧檯上的智慧型手機。老闆循線找到該名外籍老師及失竊手機，並報警處理。

外籍老師謊稱只是幫忙保管手機，等待失主與其聯繫，但法官認為依其學經歷，應可判斷手機為店員遺留吧檯，保管之說不足採信，因而認定他的竊盜犯行。

【摘自自由時報 2014.07.30】



安全管理

...

- 智慧型手機大掃除
- 學習辨識安全的 Apps
- 其他安全管理事項



進行智慧型手機大掃除

...

- 更新手機下載 App 的設定
- 改密碼
- 解除安裝沒使用的 Apps
- 檢查已下載 Apps 的授權許可
- 備份手機的聯絡人與照片



更新手機下載 App 的設定



絕對不勾選

● 43



改密碼

- 更改常使用服務的密碼(FB, LINE, Gmail...)
- 將重要服務的密碼更改為獨一無二。

- 你同時在工作電腦、家裡電腦、智慧型手機、平板電腦上登入了幾個帳號 (電子郵件、社群網路、傳訊服務.....)



● 44



解除安裝沒使用的 Apps



臺灣的智慧型手機使用者，平均下載 30 個 Apps，其中只有 9 個為經常使用的 Apps

資料來源：Our Mobile Planet (Google)

製圖：NII 產業發展協進會

手機中若安裝過多的 Apps，不但耗費電力、記憶體空間，也可能會有安全方面的疑慮。



● 45



檢查已下載 Apps 的授權許可

(Android 專用)

- 安裝 Apps 後可以在 [設定] 選單檢閱該 Apps 可使用的權限
 - 開啟 [設定] 主選單
 - 選取 [應用程式] 或 [應用程式管理員]
 - 選取應用程式
 - 向下捲動至「權限」部分

若此為 MP3 播放器 App 所要求權限，可考慮將該 App 移除。

越來越多 Apps 要求位置資訊，例如免費 Apps 伴隨的廣告，廣告平台會要求用戶位置資訊來進行更精準的行銷。



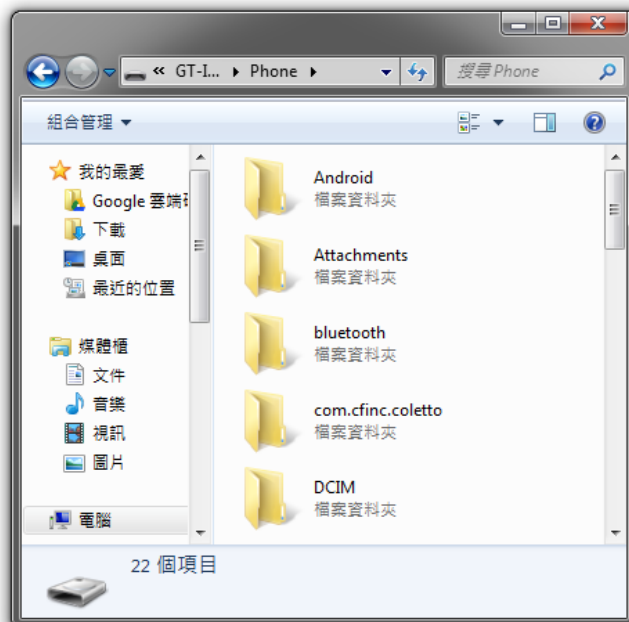
● 46



備份手機的聯絡人與照片 (1/3)

(Android專用)

- 利用 MTP 模式備份手機中的照片與其他檔案



47



備份手機的聯絡人與照片 (2/3)

(Android專用)

- 常見資料夾

Android	絕大部分軟體所需要的資料包都會存在於此
Bluetooth	藍芽傳輸的檔案存檔資料夾
DCIM	手機的相機所拍攝的照片、錄影的影片檔案存檔資料夾
Download	從網路下載檔案的預設資料夾
Pictures	內含數個資料夾，像是螢幕截圖會存放在此資料夾下；其他Apps的照片亦有可能在此，例如Instagram, Line 的影音檔案等
Whatsapp	WhatsApp 自動備份的聊天紀錄、傳輸的圖片/影片等檔案存檔資料夾。

48



備份手機的聯絡人與照片 (3/3)

(Android專用)

- 利用匯出功能備份手機中的聯絡人資訊



● 49



學習辨識安全的 Apps

...

● 50



應提高警覺的隱私相關權限

(Android專用)

權限	說明
位置	允許 App 透過手機的網路或 GPS 等方式，來取得使用者的約略位置或精確位置。
需要付費的服務	允許 App 撥打電話號碼、簡訊給特定對象
您的帳戶	允許 App 存取手機上的Google帳戶、密碼
身分識別	允許 App 使用手機上的帳戶及/或個人資料的資訊，例如讀取、修改用戶的聯絡名片內容。
聯絡人/日曆	允許 App 可使用手機的聯絡人及/或日曆資訊，例如讀取、修改用戶的聯絡人資訊；讀取日曆活動與機密資訊；在未經擁有者同意的情況下新增或修改日曆活動，以及傳送電子郵件給邀請對象

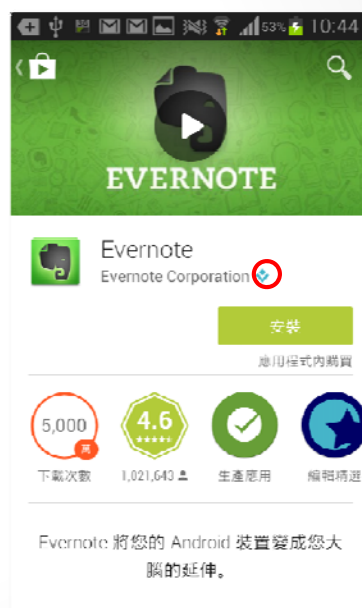
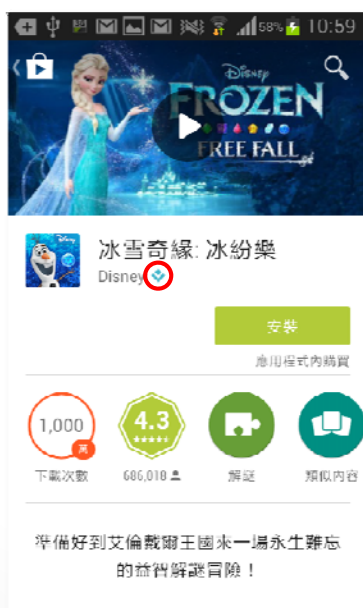
參考資料：「Google Play」說明中心

● 51



判斷 App 開發者是否有惡意嫌疑

- 若 App 獲得  頂尖開發人員 標籤，信任度上多少已有加分的參考價值。



圖案來源：Google Play

● 52



判斷星等與評論

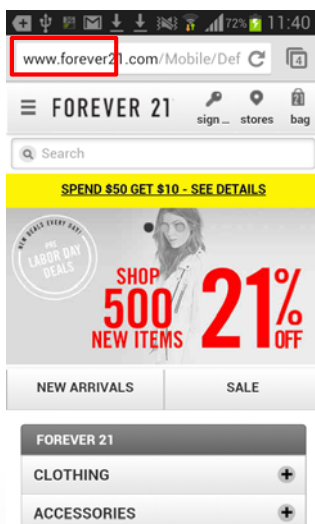
- 注意該 App 的星級評價
 - 若大家給的星等都很低，可能代表這個 App 不好用
 - 高星等的 App 也不一定都是沒問題的，應該要注意給評人數，若只有 10 個人說這個 App 有 5 顆星，參考價值可能就不高
 - 觀察使用者對該 App 之評論
 - 注意是否有使用者提出受騙等控訴之言論
 - 注意是否有大量的用戶評論都是相同且簡單的文字，可能是開發商雇用工讀生創帳號並複製貼上留言
- Apptentive 工具分析，許多 App 評價都是人工或系統產生，App Store 內有55%的假評論，Google Play 上則有45%的假評價。其中「遊戲」類占最大宗，占整體的41%。
- 多參考負面評價

53



其他安全管理事項 (1/3)

- 確保您的手機螢幕保持鎖定。
- 為手機經常造訪網站建立書籤，降低造訪釣魚網站機會。
- 當利用手機瀏覽器輸入個人敏感資料時（特別是登入網路銀行等金融服務、或輸入信用卡資訊），務必注意該網站的真實性、並確認有安全加密傳輸。



54



其他安全管理事項 (2/3)

- 不使用的時候，關閉藍牙。
- 收到簡訊、或 Line / WhatsApp/FB 即時訊息中包含 Apps 下載網址或其他網址超連結時，勿輕易點選。
- 可疑短網址分析工具。



網址掃描器	結果
ParetoLogic	Malware site
Web Security Guard	Phishing site
ADMINUSLabs	Clean site
AegisLab WebGuard	Clean site
AlienVault	Clean site
Antiy-AVL	Clean site
AutoShun	Unrated site

● 55



其他安全管理事項 (3/3)

- 加密隱私資料
善用手机資料加密服務。
- 瞭解越獄 / 解鎖裝置的風險
解鎖或越獄(Root)手機裝置會解除系統的安全防護功能。
- 刑事局開放 0911-511-111 專碼幫民眾分析可疑惡意簡訊
為蒐集分析惡意簡訊，民眾收到含有短網址的陌生簡訊可轉發至該專碼（每則訊息轉發收費約1至3元），由刑事局協助分析判別並將結果回覆給民眾。

● 56



引用圖片

編號	來源
圖片1	JeanbaptisteM , 創用CC「姓名標示 2.0」通用版, 來自Flickr網址 https://www.flickr.com/photos/jeanbaptistem/8313676753
圖片2	Ted Eytan , 創用CC「姓名標示-相同方式分享 2.0」通用版, 來自Flickr網 https://www.flickr.com/photos/taedc/9467125459
圖片3	Max Braun , 創用CC「姓名標示-相同方式分享 2.0」通用版, 來自Flickr網址 https://www.flickr.com/photos/maxbraun/12214186874
圖片4	Andresmh , 創用CC「姓名標示-相同方式分享 2.0」通用版, 來自Flickr網 址 https://www.flickr.com/photos/amonroy/6708636787/
圖片5	Mechatronics Guy , 創用CC「姓名標示 2.0」通用版, 來自Flickr網址 https://www.flickr.com/photos/38462165@N05/6038187594
圖片6	rpavich , 創用CC「姓名標示 2.0」通用版, 來自Flickr網址 https://www.flickr.com/photos/rpavich/14790943537
圖片7	University of Central Arkansas , 創用CC「姓名標示-非商業性-禁止改作 2.0」通用版, 來自 Flickr網址 https://www.flickr.com/photos/ucentralarkansas/14929011085

● 57



The end !

NII 產業發展協進會

☎ (02) 2508-2353

✉ 台北市松江路 317 號 7 樓



本簡報內容著作權為NII產業發展協進會所有

● 58