智慧型手機安全管理

2014.10.08

梁理旋
NII 產業發展協進會
☏ (02) 2508-2353
✉ 臺北市松江路 317 號 7 樓

本教材取自於教育部103年度提升校園資訊安全服務計畫
國中小學資安認知及資安推廣活動種子教師巡迴教育訓練課程
本簡報內容著作權為NII產業發展協進會所有

大綱

1. 行動通訊相關發展
2. 近期常見威脅案例
3. 智慧型手機安全管理
4. 教育部「 103 年度資安防護學園」活動說明

行動通訊相關發展

- 整體網路發展趨勢（使用者統計、使用裝置、使用行為）
- 臺灣民眾行動上網（上網行為）

High-Level User / Usage Trends*

- **Internet Users**
  <10% Y/Y growth & slowing...fastest growth in more difficult to monetize developing markets like India / Indonesia / Nigeria

- **Smartphone Subscribers**
  +20% strong growth & slowing...fastest growth in underpenetrated India / Brazil / Indonesia

行動通訊使用
高成長

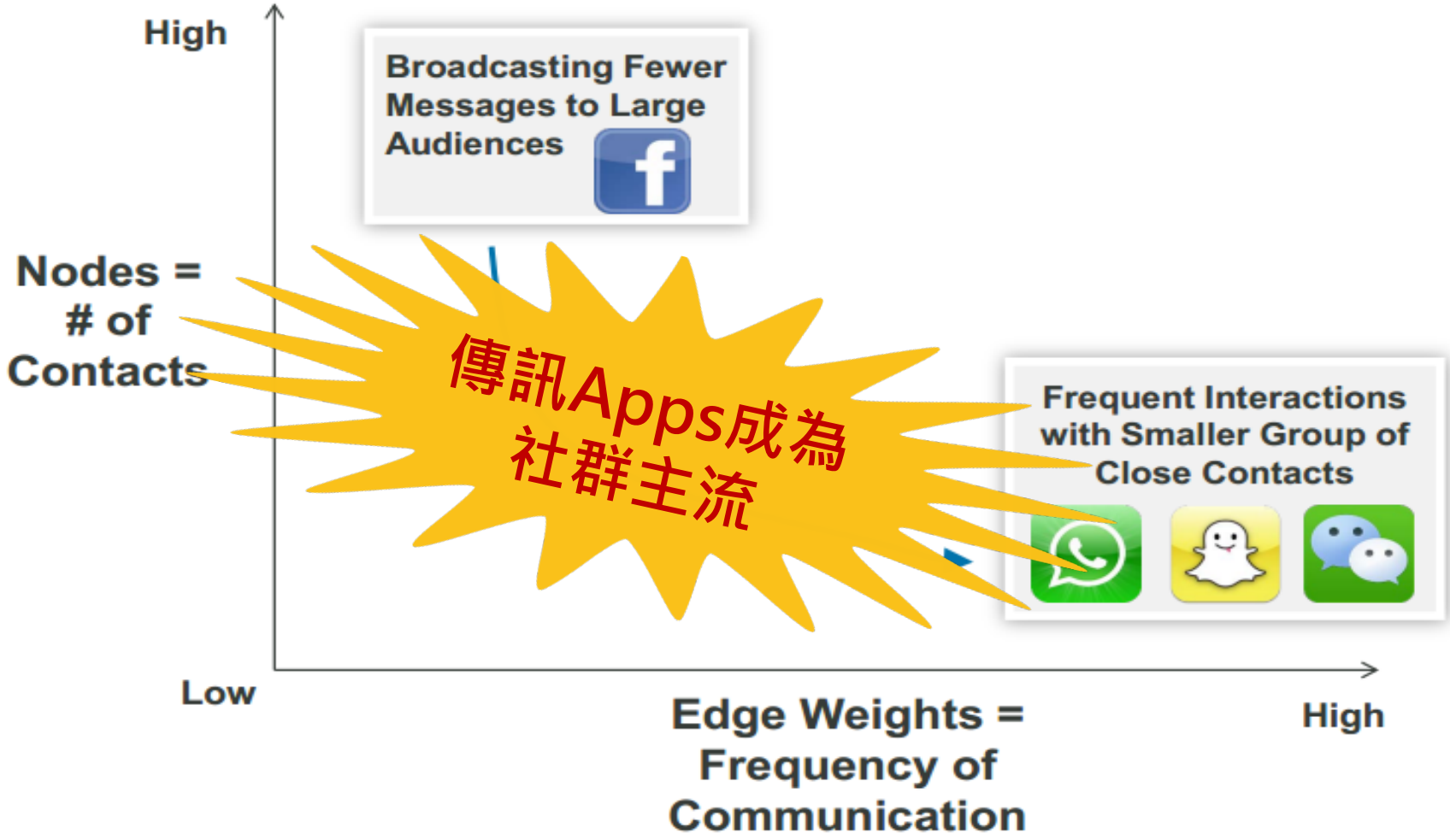
- **Tablets**
  +52% early stage rapid unit growth

- **Mobile Data Traffic**
  +81% accelerating growth...video = strong driver

@KPCB *Details on Internet Users & Smartphone Subscribers in Appendix. Source: Tablet growth per Morgan Stanley Research, 5/14. Mobile traffic per Cisco Visual Networking Index, 5/14.

資料來源：Mary Meeker, May 28, 2014, kpcb.com/InternetTrends

Evolution of Messaging → New Social Graphs... Edges = Potentially More Value than Nodes...



@KPCB Source: Anjney Midha, KPCB Associate; Jared Morgenstern, KPCB Entrepreneur Partner.

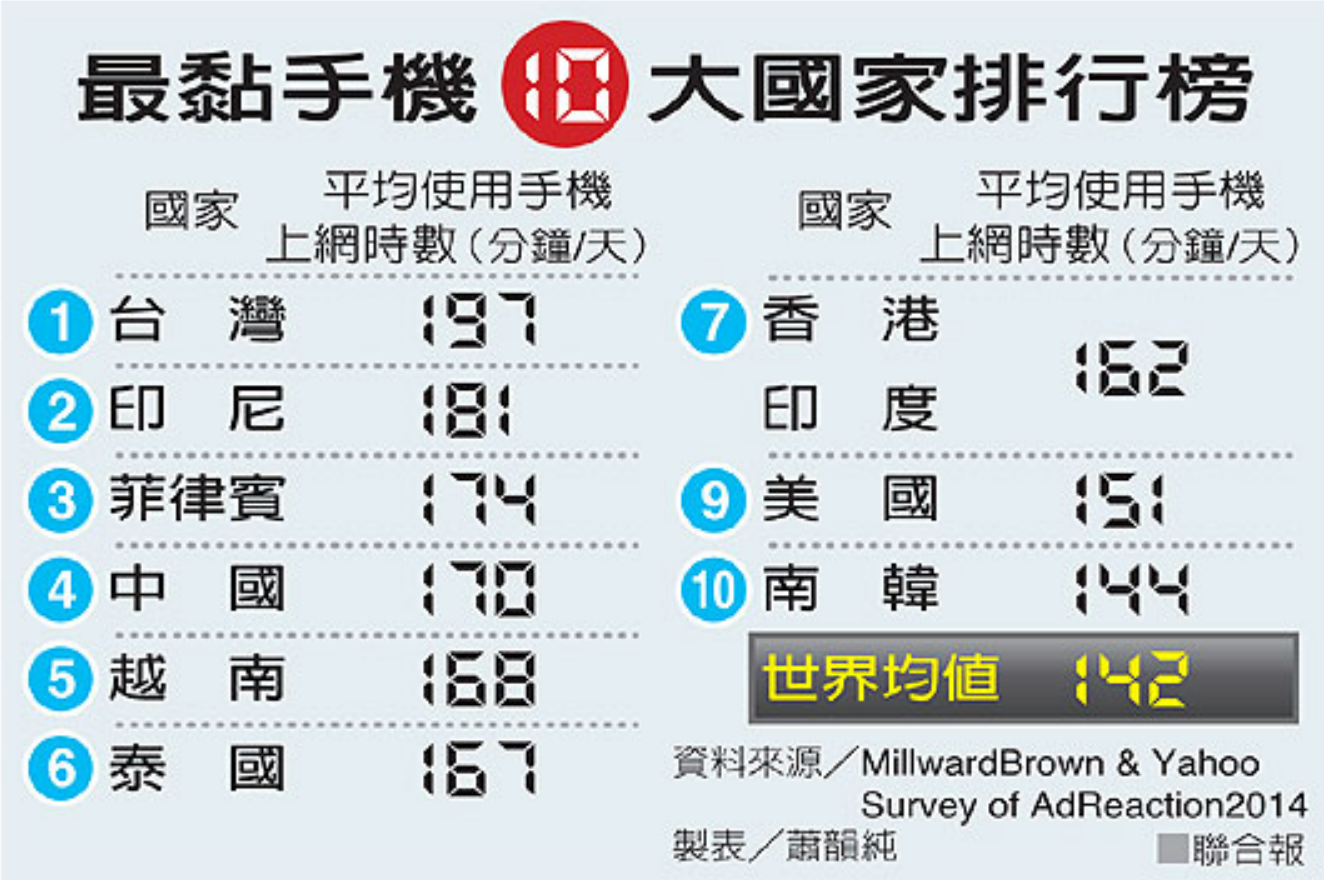
資料來源：Mary Meeker, May 28, 2014, kpcb.com/InternetTrends

Web Trends

1. 自拍
2. 新聞從 Twitter 開始
3. Internet memes

資料來源：Elise Moreau, 10 of the Most Current Trends on the Web
右方圖片來源： Ellen DeGeneres' Twitter

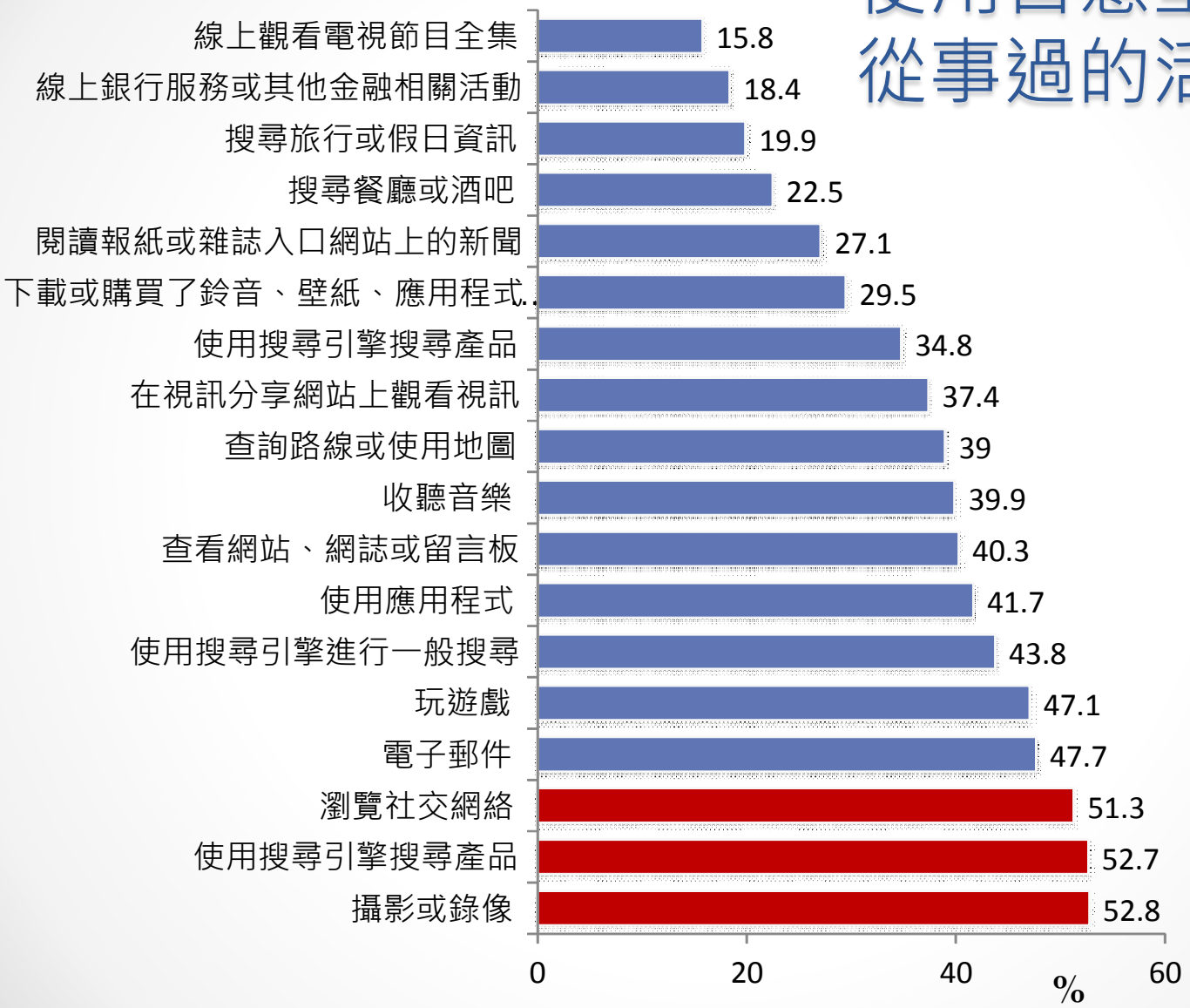
臺灣民眾愛用手機上網



圖／聯合報

資料來源：聯合報

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

近期常見威脅案例

…

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

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

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

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

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

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

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

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元的網絡支付，如非本人操作請加載電子憑證確認取消…」

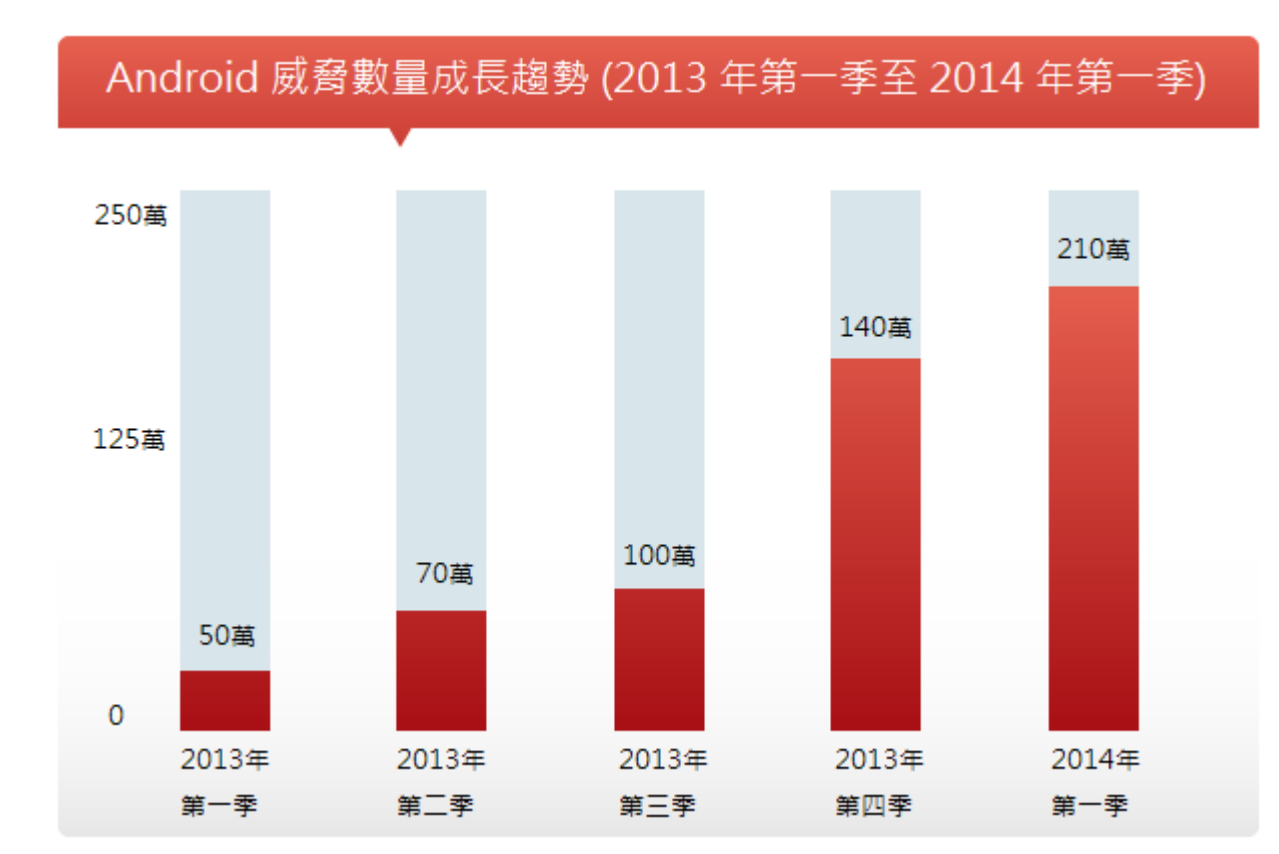
#	時事
1	「您正在申請網上支付103年○月電費共計480元，若非本人操作，請查看電子憑證進行取消」
2	fb 免費送貼圖,把此消息轉發十五個LINE好友, 可以免費領取價值一百的貼圖表情, 領取地址…”
3	「學運受傷學生急需醫藥費！」

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

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



- 圖案來源：Trend Labs 趨勢科技全球技術支援與研發中心 http://blog.trendmicro.com.tw

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】

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)

在 Google Play 的售價 $3.99

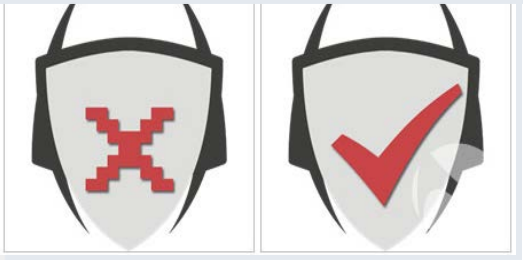
上線一週下載人次超過萬人

最高曾獲得 4.7 顆星評價

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

When I downloaded this app my phones seem to run faster

works in background and doesn't harm my battery



唯一的功能就是將 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。

參考資料：iThome，報導：Google將全額退費給Virus Shield假防毒軟體受害用戶 (2014.04.24)

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

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。

常見威脅 3.
無意間洩漏個人資料

…

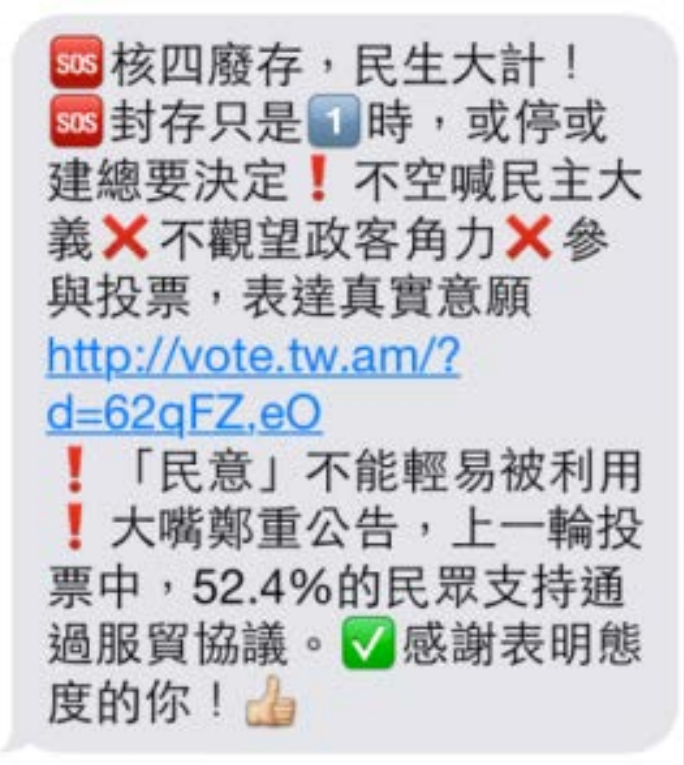
假民意調查，真個資蒐集

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】



圖案來源：阿瑪外傳 http://armorize-cht.blogspot.tw/2014/05/apple.imessage.apt.campaign.html

ookmarks Tools Help

[redacted]

导航

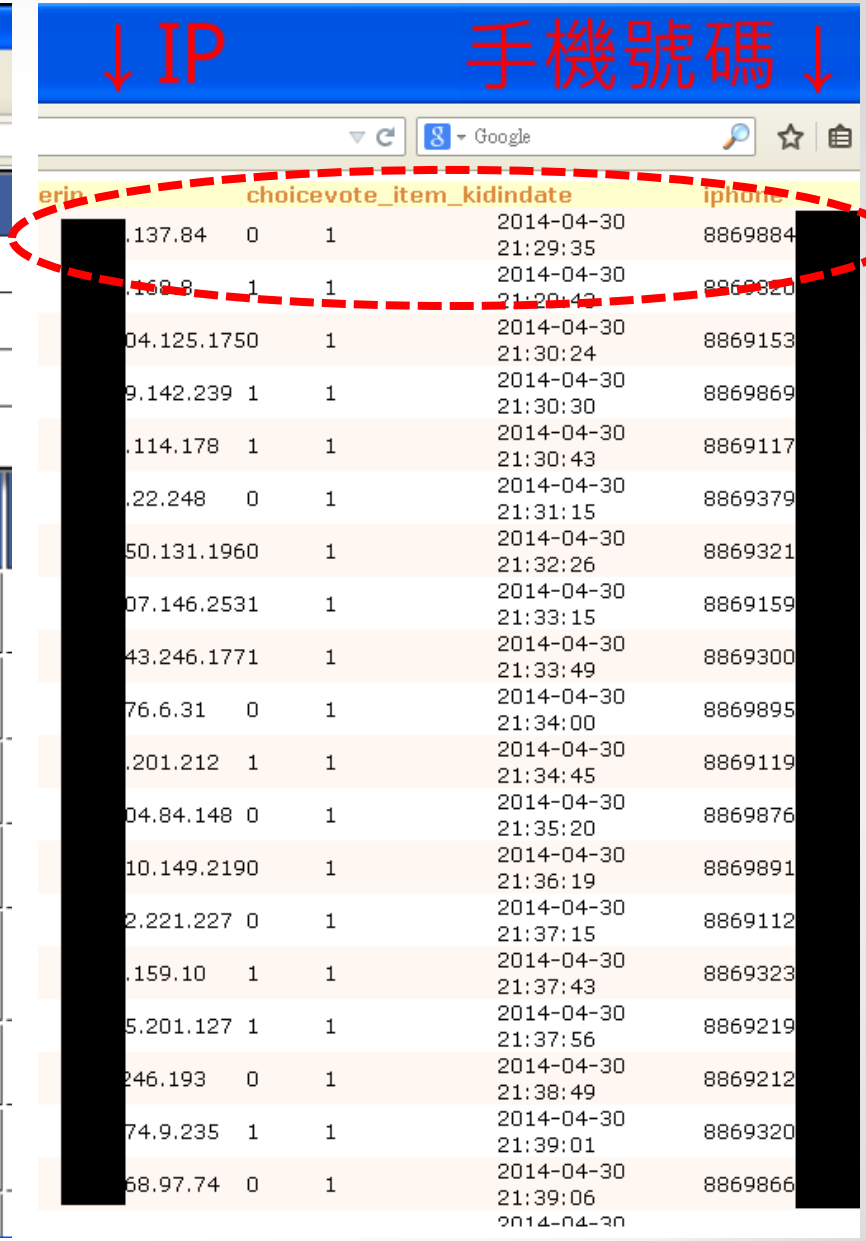
首页

用户反馈

投票记录

无号码投票记录

ip	参与投票	留言
[redacted]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。
[redacted].153	核四廢存之爭	興建核四，害子害孫。
[redacted].38	核四廢存之爭	經濟要死了
[redacted].42	核四廢存之爭	核四已建許久現今再來找議題有這必要嗎！台灣不能再虛耗時光。
[redacted].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？
[redacted].105	核四廢存之爭	安全與民生優先考慮
[redacted].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二氧化碳嗎？有電當思無電之苦
[redacted]	核四廢	[redacted]



↓IP 手機號碼↓

Google

erip		choicevote_item_kid	indate	iphone
[redacted].137.84	0	1	2014-04-30 21:29:35	8869884[redacted]
[redacted].168.8	1	1	2014-04-30 21:29:43	8868820
[redacted]04.125.1750		1	2014-04-30 21:30:24	8869153
[redacted]9.142.239	1	1	2014-04-30 21:30:30	8869869
[redacted].114.178	1	1	2014-04-30 21:30:43	8869117
[redacted].22.248	0	1	2014-04-30 21:31:15	8869379
[redacted]50.131.1960		1	2014-04-30 21:32:26	8869321
[redacted]07.146.2531		1	2014-04-30 21:33:15	8869159
[redacted]43.246.1771		1	2014-04-30 21:33:49	8869300
[redacted]76.6.31	0	1	2014-04-30 21:34:00	8869895
[redacted].201.212	1	1	2014-04-30 21:34:45	8869119
[redacted]04.84.148	0	1	2014-04-30 21:35:20	8869876
[redacted]10.149.2190		1	2014-04-30 21:36:19	8869891
[redacted]2.221.227	0	1	2014-04-30 21:37:15	8869112
[redacted].159.10	1	1	2014-04-30 21:37:43	8869323
[redacted]5.201.127	1	1	2014-04-30 21:37:56	8869219
[redacted]246.193	0	1	2014-04-30 21:38:49	8869212
[redacted]74.9.235	1	1	2014-04-30 21:39:01	8869320
[redacted]68.97.74	0	1	2014-04-30 21:39:06	8869866[redacted]
			2014-04-30	

圖案來源：阿瑪外傳 http://armorize-cht.blogspot.tw/2014/05/apple.imessage.apt.campaign.html

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到內容。

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。

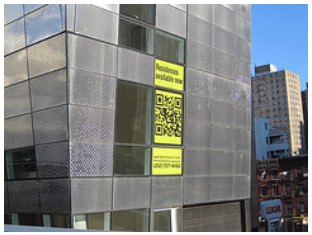
【摘自數位時代 2014.03.13】

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

…

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】

智慧型手機安全管理

- 智慧型手機大掃除
- 學習辨識安全的 Apps
- 其他安全管理事項

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

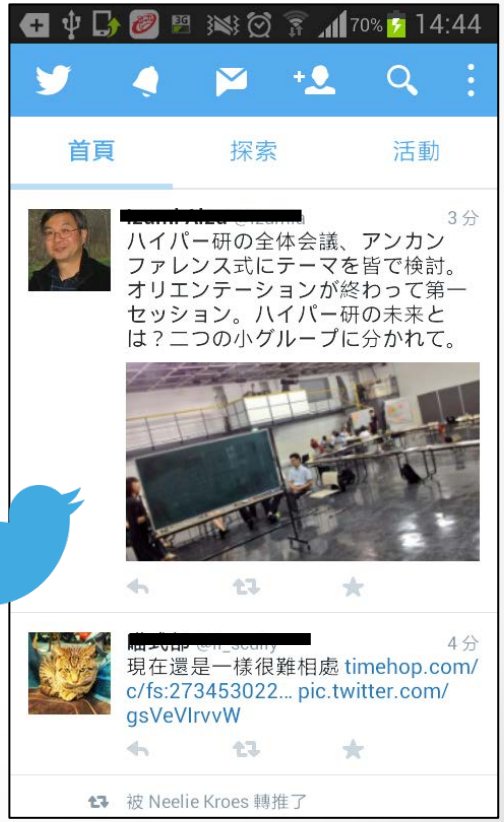
更新手機下載 App 的設定

絕對不勾選

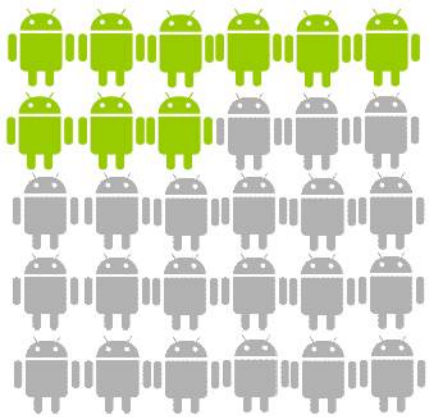
改密碼

- 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……）



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。

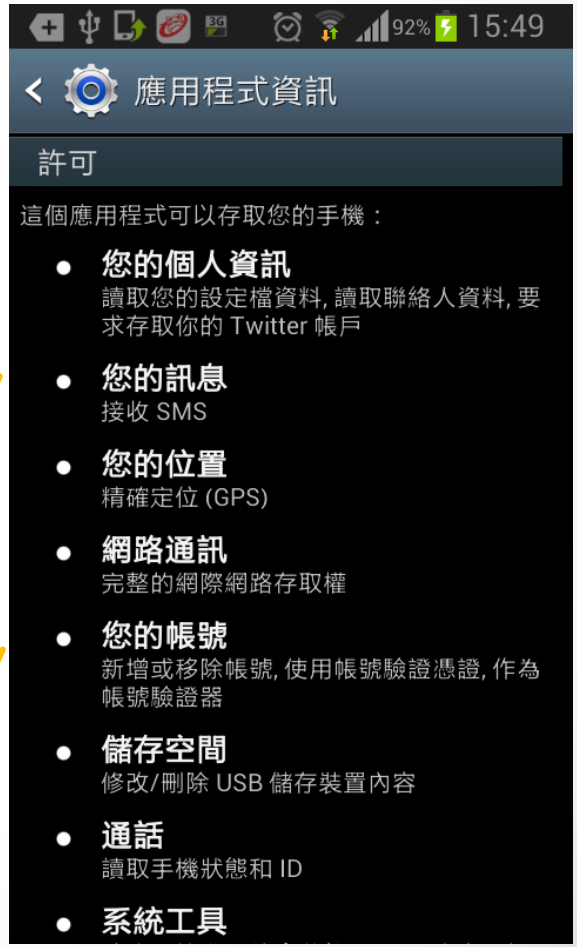
檢查已下載 Apps 的授權許可

（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。



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

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
Donload	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。

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

學習辨識安全的 Apps

…

應提高警覺的隱私相關權限

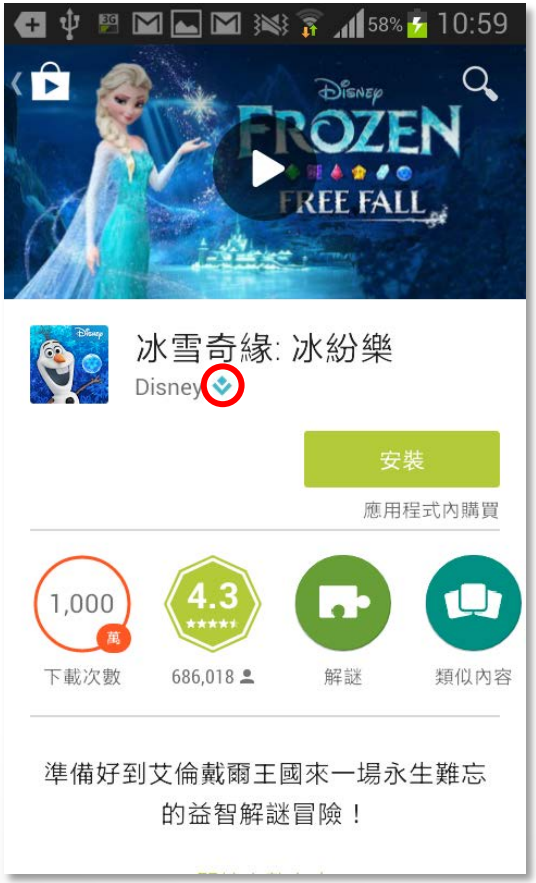
（Android專用）

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

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

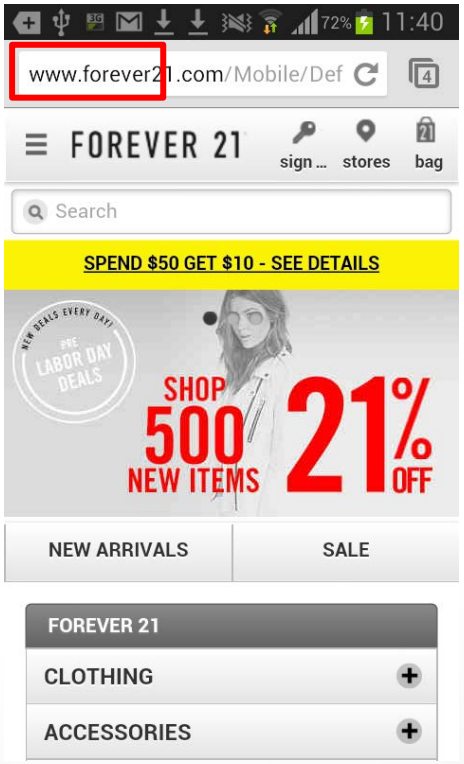
判斷星等與評論

- 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

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。



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。

其他安全管理事項 (3/3)

- 加密隱私資料

  善用手機資料加密服務。

- 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。

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

教育部「 103 年度資安防護學園」活動說明

…

活動網站首頁

網址：http://cissnet.edu.tw/safely

活動辦法

- 活動時間：103 年 10 月 1 日至 103 年 11 月 15 日止
- 活動對象：國中小學 3~9 年級在學學生
- 闖關方式：
  - 本活動共分成「3」（三、四年級）、「5」（五、六年級）、「7」（七、　八、九年級）三個組別，請學生依年級別參加。
  - 每一個組別各有 3 道關卡，每個關卡有 10 道題目。
- 每個關卡中，只要答對 6 題以上，即可獲得「挑戰資安大富翁」金幣1枚（可以累積 1 次抽獎機會），累積愈多金幣中獎機會就愈大！（每位同學最多可累積**45次**抽獎機會）
- 使用OpenID帳號登入參加本活動的同學，就有機會抽中OpenID獎。
- 各組別「參與率最高」的前2名或第1名縣市，將抽出1個班級頒發「班級團體獎」。

班級團體獎

各級別由參與率最高的前2名或第1名縣市中抽出1個得獎班級。

級別	抽獎級距	符合條件的縣市數	得獎名額
3~4年級	班級數400班以上	14	2名
	班級數未達400班	8	1名
5~6年級	班級數400班以上	14	2名
	班級數未達400班	8	1名
7~9年級	班級數500班以上	15	2名
	班級數未達500班	7	1名

參與率計算方式：
各級別不重覆闖關成功人次數量（每個帳號不管闖幾關都只能計算1人次）÷
各級別縣市學生數（以教育部統計處102年度各級學校縣市別學生數為計算基礎）

參與率排行榜1

各抽出1個得獎班級。
從各級別參與率前2名的縣市中，

縣市	3~4年級班級數
新北市	2704
臺中市	2175
高雄市	1958
桃園縣	1744
臺北市	1624
臺南市	1380
彰化縣	1057
屏東縣	731
雲林縣	625
苗栗縣	528
新竹縣	522
南投縣	518
嘉義縣	485
宜蘭縣	415

縣市	5~6年級班級數
新北市	2927
臺中市	2333
高雄市	2095
桃園縣	1846
臺北市	1822
臺南市	1448
彰化縣	1122
屏東縣	790
雲林縣	665
南投縣	566
苗栗縣	555
新竹縣	515
嘉義縣	513
宜蘭縣	429

縣市	7~9年級班級數
新北市	4128
臺中市	3457
高雄市	3183
臺北市	2812
桃園縣	2696
臺南市	2206
彰化縣	1548
屏東縣	1012
雲林縣	876
新竹縣	712
苗栗縣	708
南投縣	695
宜蘭縣	640
新竹市	592
嘉義縣	537

參與率排行榜2

從各級別參與率第1名的縣市中，抽出1個得獎班級。

縣市	3~4年級班級數
新竹市	381
花蓮縣	347
基隆市	274
臺東縣	269
嘉義市	223
澎湖縣	109
金門縣	64
連江縣	16

縣市	5~6年級班級數
新竹市	386
花蓮縣	357
基隆市	295
臺東縣	287
嘉義市	232
澎湖縣	120
金門縣	65
連江縣	18

縣市	7~9年級班級數
基隆市	453
花蓮縣	451
嘉義市	394
臺東縣	317
澎湖縣	130
金門縣	80
連江縣	18

活動獎項

- 三至九年級學生，共分成三組，每組皆可獲得獎項。
- 獎項除了規劃普遍受到學生族群歡迎的3C電子產品之外，為鼓勵學生多花點時間與家人朋友互動，亦挑選適合親朋好友同樂的桌遊類型獎品。

組別	獎項	名額	獎勵
3/5/7年級	頭獎	各組1名	7吋平板電腦
	二獎	各組2名	樂高積木
	三獎	各組3名	地產大亨桌遊
	四獎	各組10名	UNO疊疊樂
	五獎	各組15名	便利超商禮券200元
	班級團體獎	各組3名	便利超商禮券2,000元
	OpenID獎	各組10名	便利超商禮券 500

抽獎及領獎方式

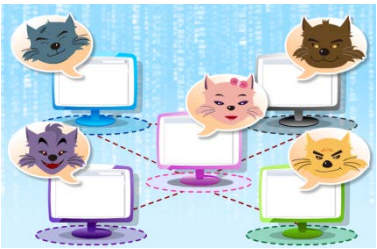
- 抽獎方式：
  - 預計 103 年 11 月底公開抽獎。
  - 每一位參加的同學只有一次中獎機會。
  - 得獎名單將於 12 月中旬前公告於活動網站。

- 領獎方式：
  - 主辦單位會在抽獎活動結束後 2 個月內和得獎同學的指導老師聯絡，並和老師確認得獎同學的身分後，再將獎品寄到學校，由指導老師將獎品頒給得獎同學。
  - 「班級團體獎」也會寄到學校交給指導老師。

我要看動畫

- 依據三個級別，分別提供三支動畫。
- 提供「線上瀏覽」及「檔案下載」功能。

本年度教材主題

3~4年級	網路安全守則 - 非禮勿視	網路安全守則 - 非禮勿言	網路安全守則 - 非禮勿動
5~6年級	行動裝置使用叮嚀	行動裝置安心遊網	行動裝置App活用
7~9年級	 網路交友三思而後行	網路留言三思而後寫	網頁連結三思而後點

我要充電

- 依據三個級別，分別提供三則充電內容。
- 充電內容可搭配動畫教材進行延伸學習。

我們的成績單

- 依據三個級別，提供「縣市參與率排行榜1」及「縣市參與率排行榜2」
- 各縣市學生數資料來源：教育部統計處102年度各級學校縣市別學生數

我們的成績單

縣市排行榜

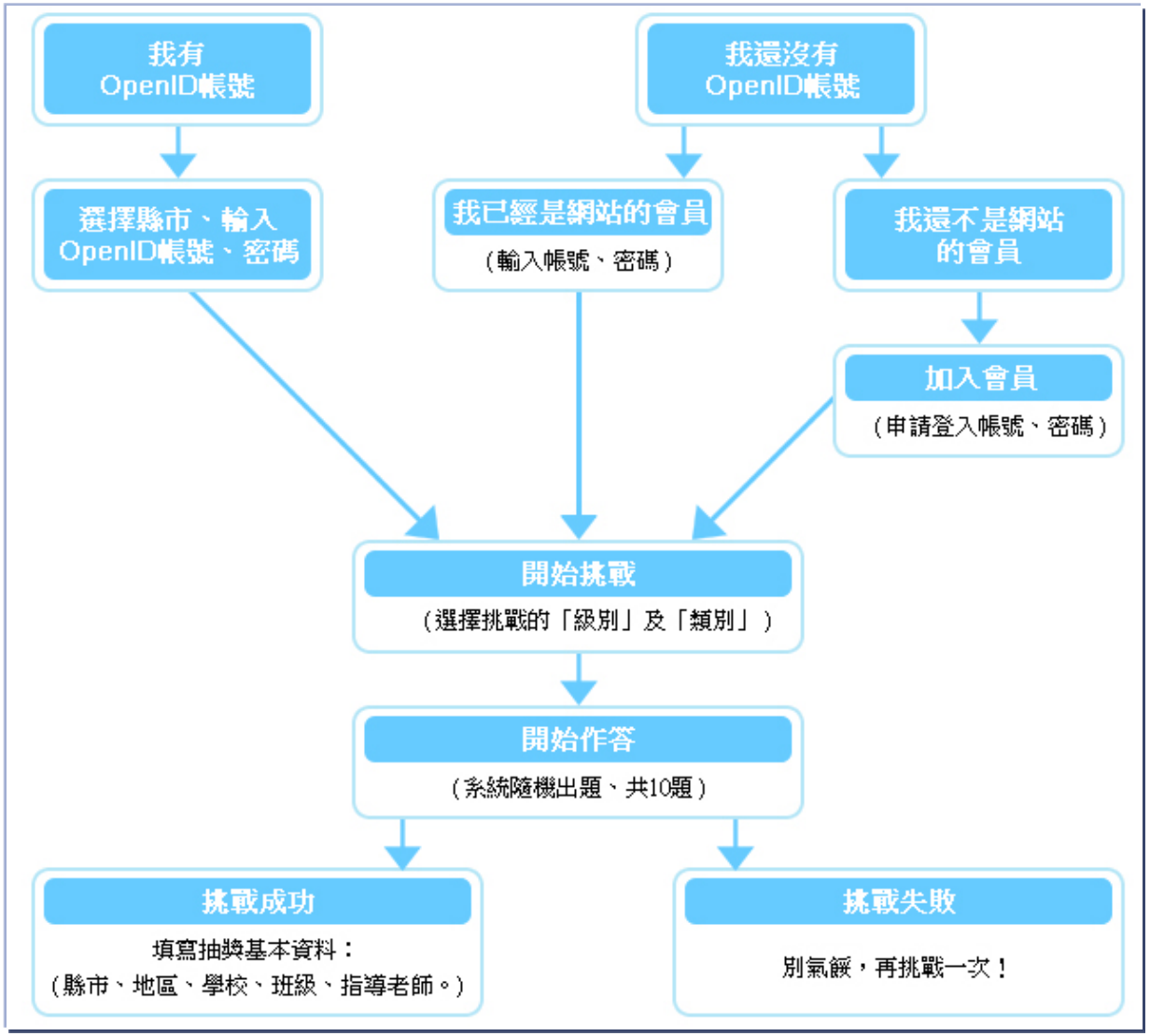
級別：3 (適用於國小3、4年級)

縣市參與率排行榜1　縣市參與率排行榜2

最後更新時間：2012/10/15 17:00:00

名次	縣市	闖關成功人次數量	該縣市學生數	縣市參與率
1	雲林縣	52110	49055	181.26%
2	台北市	49055	38751	133.95%
3	高雄市	38751	52110	84.14%
4	基隆市	52110	49055	181.26%
5	新竹市	49055	38751	133.95%
6	台中市	38751	52110	84.14%
7	雲林縣	52110	49055	181.26%
8	台北市	49055	38751	133.95%
9	高雄市	38751	52110	84.14%
10	基隆市	52110	49055	181.26%
11	新竹市	49055	38751	133.95%
12	台中市	38751	52110	84.14%
13	雲林縣	52110	49055	181.26%
14	台北市	49055	38751	133.95%

檢測流程


我有
OpenID帳號
我還沒有
OpenID帳號
選擇縣市、輸入
OpenID帳號、密碼
我已經是網站的會員
（輸入帳號、密碼）
我還不是網站
的會員
加入會員
（申請登入帳號、密碼）
開始挑戰
（選擇挑戰的「級別」及「類別」）
開始作答
（系統隨機出題、共10題）
挑戰成功
填寫抽獎基本資料：
（縣市、地區、學校、班級、指導老師。）
挑戰失敗
別氣餒，再挑戰一次！

登入方式（有OpenID）

使用OpenID登入（以基隆市為例）

基隆市教育網路單一帳號入口網
& OpenID Server

openid.kl.edu.tw OpenID

首頁 登錄

用戶登入

用戶名: ag0000

密 碼: ••••••••••••

登錄

基隆市教育網路單一帳號入口網 & OpenID Server 基隆市教育處

openid.kl.edu.tw OpenID

首頁 個人資料 站點管理 服務 退出登錄 新帳號邀請

當前登錄用戶： *ag0000*

您是否確定要使用您的 OpenID URL (http://openid.kl.edu.tw/u/ag0000) 登錄到站點 http://cissnetactivity2014.test.demo2.miniasp.com.tw/?

http://cissnetactivity2014.test.demo2.miniasp.com.tw/ 同時請求獲取您在這裡保存的某些個人檔案信息。以下是將被發送給對方的信息（包括必填和可選字段）：

發送?	信息名稱	信息內容	狀態
☑	暱稱(Nickname)	Test	必填
☑	全名(Full Name)	測試帳號	必填

您可以修改「發送?」欄的復選框狀態來決定發送給對方哪些信息。

該站點尚未提供任何用戶策略信息.

確定 永久確定 拒絕請求 選擇「確定」或「永久確定」後該站點將出現在您的「站點管理」界面中，您可以隨時調整信任策略。

基隆市教育網路單一帳號入口網 & OpenID Server 基隆市教育處

資安防護學園
挑戰資安大富翁
::: 回首頁 | 網站地圖 | 校園資訊安全服務網 | 教育部網站 | OpenID相關問題
會員專區
會員登入 | 加入會員
首頁
活動辦法
活動獎項
我要看動畫
我要充電
我要挑戰
我們的成績單
獎落誰家
教學教案
您現在的位置是：首頁 > 挑戰資安防護學園 > 會員登入
會員登入
網頁訊息
歡迎登入資安防護學園～馬上進入挑戰頁面！
確定
基隆
新竹縣
新竹市
苗栗
雲林縣
嘉義縣
嘉義市
台南市
高雄市
屏東縣
台東縣
花蓮縣
宜蘭縣
澎湖縣
金門縣
連江縣

登入方式（沒有OpenID）

加入會員

- 填寫「帳號」、「密碼」、「Email」（非必填）。
- 閱讀「活動參與同意書」與「隱私權政策」。
- 注意事項：
  - 帳號長度：至少 6 個字元。
  - 輸入帳號後，若資料庫中已有相同的帳號，會有提示訊息。
  - 帳號與密碼不能相同。
  - Email 非必填欄位！
    Email 使用時機：當您忘記密碼時，寄送密碼通知函。

選擇挑戰級別及關卡

- 成功加入會員後，系統導引至「我要挑戰」。
- 依據三個級別，各有三個關卡。

開始挑戰

- 每個級別共有 3 個主題的挑戰關卡，每個關卡各有 10 個題目，每題 1 分。
- 答對 6 題（含）以上，就可以獲得「挑戰資安大富翁」金幣 1 枚！（可以累積一次抽獎機會）
- 挑戰成功，填寫抽獎資訊，作為確認抽獎身分之依據。

列印獎狀

- 三個關卡全部過關，「列印獎狀」的功能鈕就會亮起來，可以將資安大富翁的榮譽列印出來。
- 老師在課堂上帶領同學進行檢測時，可透過「列印獎狀」來確認同學是否完成檢測。

教學進行時連線異常處理方式

- 請至「校園資訊安全服務網」(http://cissnet.edu.tw)之「國中小資安推廣」專區下載「教學教案」及「動畫教材」，進行離線教學。
- 動畫教材位置：http://cissnet.edu.tw/Learn/LearnAnimation
- 教學教案位置：http://cissnet.edu.tw/Learn/LearnCase
- 建議老師可事先開啟測驗頁面備用，即可直接廣播公布題目，請學生利用紙張作答，與老師互動及討論。
- 進行通報作業：
  - 電話：(02)2508-2353#140或331
  - 電子郵件：cissnet@nii.org.tw

簡報完畢，敬請指教

本簡報內容著作權為NII產業發展協進會所有