投稿類別：資訊類

篇名：

探討高中職生對手機行動裝置資訊安全使用因素之探討

作者：

李博仁。私立樹德高級家事商業職業學校。職高資處科 3 年 12 組

林琦紘。私立樹德高級家事商業職業學校。職高資處科 3 年 12 組

葉子維。私立樹德高級家事商業職業學校。職高資處科 3 年 12 組

指導老師：

施玉情老師

壹●前言

一、研究背景

科技的進展，的確帶給人們許多方便及生活品質的提升。但是技術上的一些不足或有心人士的刻意，也引發了一些安全的問題。例如，無線網路很方便，但一般民眾不瞭解或沒有作安全防護，機密資料就很容易洩漏。最近網路上盛傳一種可以破解無線網路密碼的產品，有此寶物，只要電腦可以收到無線網路的訊號，即可免費連線使用。這些都是網路普及後所帶來的一些問題，愈瞭解，對網路使用就愈保守。

舉例而言，2004 年研究人員發現手機病毒 Cabir。此病毒會自動搜索周圍安裝有藍牙功能的諾基亞特定型號的智慧型手機，並不斷地將惡意程式自動發送給任何它搜尋得到的藍牙手機。然而此病毒對手機危害並不大，遭受感染的手機僅會在螢幕上出現「Caribe」字樣，也因為其會不斷地進行附近藍牙手機的搜索，導致縮短手機電池待機時間。

二、研究動機

以未來發展趨勢來看，由於微軟在智慧型手機作業系統市場著力相當積極，而且其因與個人電腦的作業系統類似，可複製使用者在個人電腦的應用經驗並降低學習時間。加上微軟不斷結合其多元化數據應用程式的優勢，並在版本上推陳出新，以及與手機製造商緊密的合作與互動，已逐漸在智慧型手機作業系統上普及。

而且，隨著手機可以支援無線區域網路如 Wi-Fi 或 WiMAX，或透過 3G、3.5G 網卡直接上網瀏覽網頁或收發電子郵件，傳統在個人電腦可見的安全威脅，都將可能在手機上出現，手機病毒造成的安全威脅，將變得更加複雜且難以預測！

三、研究目的

本研究主要目的在探討高中(職)生使用手機資訊安全裝置的因素，主要目的是希望從高中職生對手機行動裝置資訊安全之使用，研究目的在探討影響高中職生採用手機資訊安全裝置的決定因素。本研究的研究目的，主要分為以下幾點：

1、手機行動資訊安全裝置的系統品質對使用意願有影響

2、手機行動資訊安全裝置的有用性對使用意願有影響

貳●正文

一、文獻探討

(一)行動安全認知差異大僅16%使用者安裝防護軟體

智慧型手機、平板電腦等可攜式連網裝置大受消費者歡迎，也成為網路犯罪歹徒眼中的新興市場，但大多數使用者卻沒有意識到行動安全問題的嚴重性。

在諾頓報告中還有幾個調查數字，說明了民眾對網路安全的認知，與實際行動間的落差：74%的受訪者表示知道網路犯罪的存在，但卻沒有採取任何必要的防範措施41%的成年受訪者缺乏一套隨時保持更新的完整安全軟體來保護其個人資訊在網路上的安全性不到一半(47%)的人會定期檢閱其信用卡帳單來查看是否遭到盜刷有61人未使用複雜的密碼，也未定期更改密碼在透過手機上網的族群當中，只有16%安裝了最新的行動裝置安全軟體。在這個生活離不開網路的年代，如何教育市場，讓使用者認知到網路安全的重要性，並願意採取相對應保護措施，不只是資安廠商與政府的課題，也是新興科技研發者的責任。

(二)逾半數用戶缺乏對智慧型手機的安全認知

網路安全軟體公司BullGuard日前發現，有超過半數的用戶並不清楚智慧型手機的資訊安全議題。

在調查當中，有21%的受訪者相信資訊安全保護是多餘不必要的，另有42%的受訪者承認他們從未想過資訊安全的議題。而其他調查發現，49%的受訪者並未考慮使用手機連結至網際網路，另有32%的受訪者表示並未想到當中可能具備的潛在風險。

另外，88%的受訪者承認他們並非“完全”地信任網際網路，相較於使用電腦連結上網際網路的途徑，僅11%的受訪者認為使用手機連結上網際網路是較安全的，有26%的受訪者持反對意見，另有31%的受訪者認為兩者一樣安全。此次調查的結果顯示了用戶們普遍缺乏對於智慧型手機資訊安全及安全風險的認知。

BullGuard的行動安全專家Claus Villumsen表示：對此次調查的結果並未感到意外，人們希望買到“可以用”的東西，但卻並不在意這項設備在運作上可能會遭遇到的環節。有一點需要謹記在心的是智慧型手機是電腦的縮小版，所以它也一樣容易受到有心者的攻擊。因此，必須教育手機用戶們在使用手機連結上網際網路、收發信件及執行財務交易時可能具備的潛在風險。

(三)手機安全裝置之分類

行動裝置的資安要求與電腦的資安要求並無二致，即為保護行動裝置的機密性、完整性及可用性：

(1)機密性意指確保傳輸與儲存之資料無法被未授權人士存取。

(2)完整性意指偵測傳輸與儲存之資料是否被有意或無意的變更。

(3)可用性意指確保使用者可透過行動裝置存取所需的資源。

為滿足以上的資安要求，行動裝置需要多項資安保護措施，以下將依軟體下載與使用、資料保護、連線功能設定及密碼設定等類別，分別提出防護建議。其中連線功能設定與密碼設定係透過行動裝置內建功能即可達成。

(四)軟體下載與使用

(1)僅安裝來自可信任來源之軟體：在行動裝置下載軟體前，除先行針對欲安裝之軟體進行安全性之基本評估。如：檢視要求權限、使用者評論等）外，請儘可能確保軟體來自於合法的官方軟體商店(如App Store、Google Play)，切勿從無法驗證其可靠性之來源下載安裝軟體，以避免安裝已遭植入非正當意圖之軟體，導致行動裝置資料遭竊、或被安裝後門程式及對行動裝置產生損害之風險。

(2)注意軟體權限：行動裝置上的軟體於安裝或在第一次使用時，大都會詢問使用者其可讀取的軟體權限，惟部分軟體會要求讀取行動裝置的地理位置(GPS)、通訊錄、通話次數及系統工具等敏感資料。因此，使用者於安裝軟體時，請注意該軟體是否要求不必要的權限。此外，軟體於更新時，大都也會重新詢問其可讀取的軟體權限，請再確認該軟體所要求的權限是否合理，再評估是否進行安裝。

(3)軟體定期更新修補程式：行動裝置上的軟體（如瀏覽器）或作業系統，可能因漏洞而遭受駭客攻擊，如，瀏覽網頁時被轉址到惡意網站或釣魚網站，造成敏感資料外洩或被植入惡意程式等資安問題。因此，行動裝置上的軟體或作業系統應定期自動或手動安裝更新修補程式。

(4)安裝資安防護軟體：為避免下載已知的惡意程式與瀏覽惡意網站，可透過安裝資安防護軟體（如防毒軟體），以偵測已知的惡意程式與惡意網站。機關可以利用行動裝置管理系統(Mobile Device Management, MDM)管理機關內的行動裝置。

MDM 主要目的在於限制行動裝置上，可以從事的行為，甚至可遠端變更

與清除行動裝置的內容，如，機關可透過MDM 發送簡訊，亦可進行要求行動裝置設置密碼、限制密碼長度、加密行動裝置內的檔案、使用軟體權限等各類政策。

二、研究設計

(一)研究架構

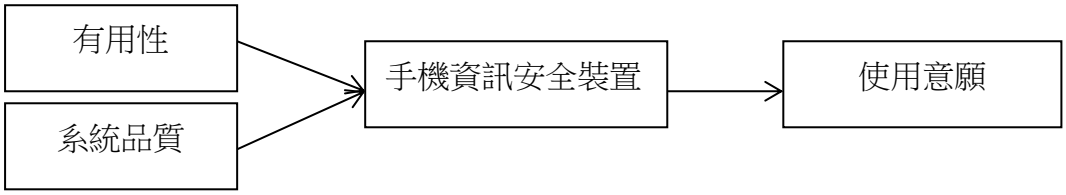

圖 1 本研究架構圖

(二)研究設計

本研究是以「探討高中職生對手機行動裝置資訊安全使用」調查問卷取得資料。此問卷主要依研究目的及文獻探討所得區位因子，加以歸納設計而成。問卷內容是由三大部分所組成：

第一部分為曾使用過智慧型手機中的行動裝置資訊安全使用者們一些基本資料調查，例如科系、年級、性別...等。第二部分則是使用者對於手機行動資訊安全的了解。第三部分則是對手機的(使用&選擇決策因素)

三、問卷結果與統計分析

(一)樣本性別分析

有效樣本中，受測者的性別比例為男性佔 61%，女性佔 39%。

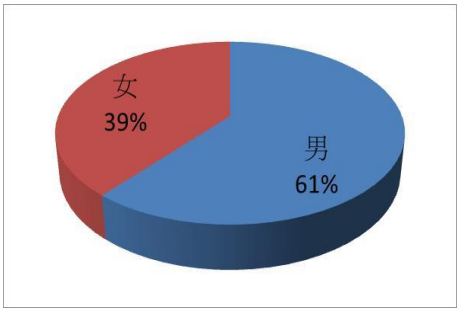

圖 2、樣本性別比例圖

(二)樣本年級比例

經過分析後，發現施測的年級比例以三年級 74%為居高。

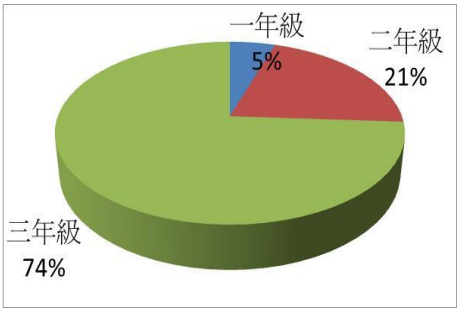

圖 3、樣本年級比例圖

(三)樣本科系比例

經過分析後發現，以資料處理科 65%為最多，其次是幼保科 11%。

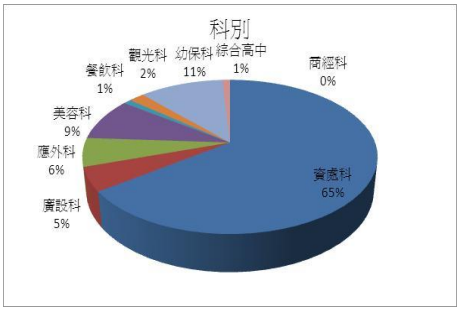

圖 4、樣本科系比例圖

(四)瞭解手機資訊安全代表什麼意義之比例

經過分析後發現，選擇可幫助手機安全性的人以 75%，其次為 25%的人選擇可增加手機執行速度。

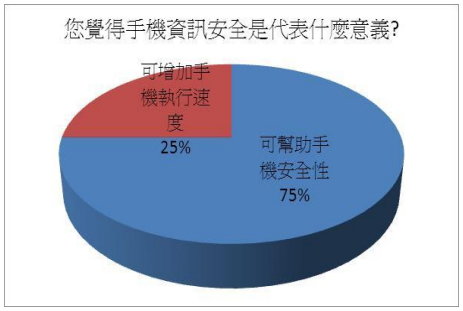

圖 5、樣本選擇意義比例圖

(五)瞭解手機資訊安全的主要動機之比例

經過分析後發現，有 35%的受測者為玩遊戲的動機最多，其次為 34%是上網。

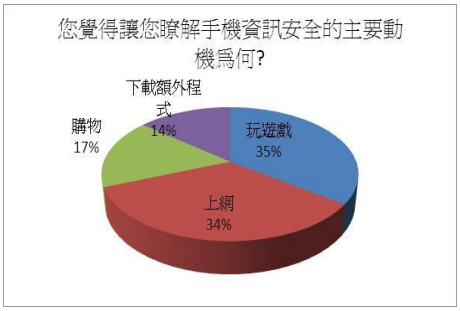

圖 6、樣本選擇動機比例圖

(六)如何得知手機資訊安全之比例

經過分析後發現，有 68%的受測者來自網際網路最多，其次為親友教導和路邊看到為 11%。

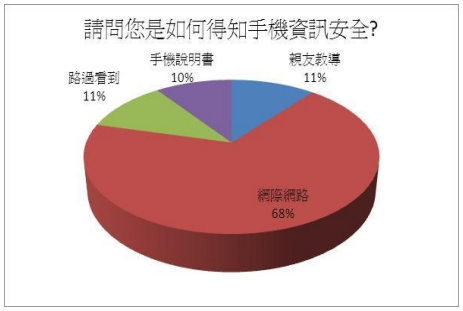

圖 7、樣本選擇得知手機安全比例圖

(七)如何使用手機資訊安全之比例

經過分析後發現，有 47%的受測者選擇安裝資訊安全軟體為最多，其次為 43%的安裝防毒軟體。

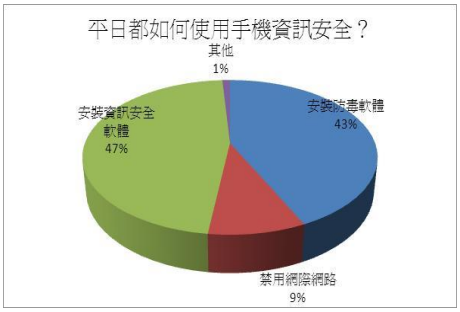

圖 8、樣本使用手機資訊安全比例圖

(八)手機安全防護裝置是必備

經過分析後發現，有 72%的受測者認為手機的安全防護裝置是必備的。

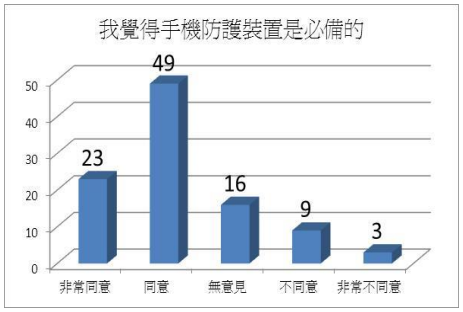

圖 9、手機防護裝置比例圖

(九)手機的防護比電腦還要精細

經過分析後發現，有 50%的受測者是認為手機的防護是比電腦還要精細的。

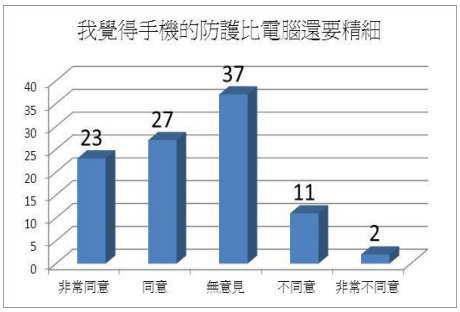

圖 10、手機與電腦精細度比例圖

(十)電腦的防護裝置與手機功能相似

經過分析後發現，有 65%的受測者認為電腦與手機的防護裝置是非常相似的。

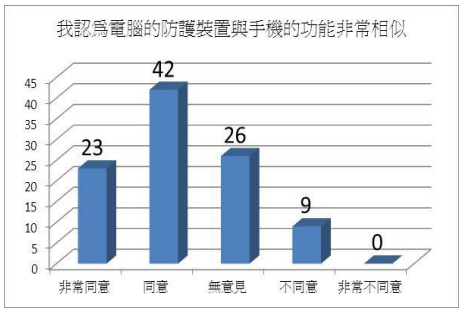

圖 11、電腦與手機的防護裝置比例圖

(十一)了解手機資訊安全是必需

經過分析後發現，有 75%的受測者認為了解手機資訊安全是必需的。

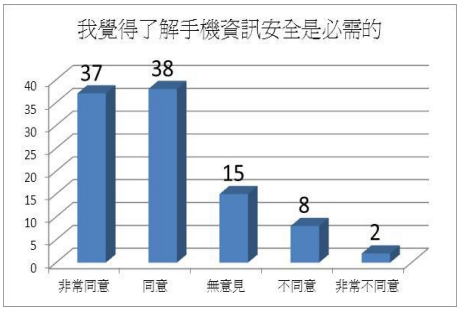

圖 12、了解手機資訊安全比例圖

(十二)因行動資訊安全而去理解它的來源

經過分析後發現，有 63%的受測者會因為行動資訊安全而去理解它的來源。

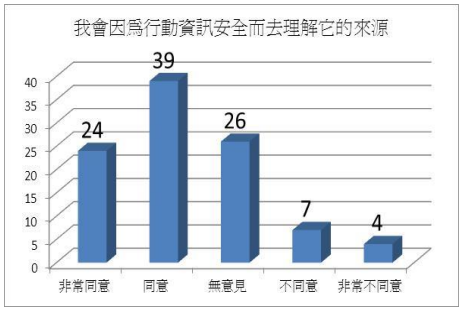

圖 13、理解行動資訊安全比例圖

參●結論

一、研究結論

行動運算已成為商業通訊常態，而行動裝置儼然成為駭客竊取資訊的新興威脅管道，若沒做好防範，駭客可在幾秒內就將如特洛伊木馬等惡意程式上傳至行動裝置，進而擷取裝置畫面上的個人資訊。

本研究發現，手機行動資訊安全裝置，隨時免費進行手機防護，行動族可不用花錢也能保障手機內的安全，現代人在生活中脫離不了的手機，在行動裝置上的防護、防毒軟體，隨著時代的演變，只要有手機，可快速得知不同的手機安全的資訊。

二、建議

(一)現代的手機功能有非常多的變化，但是其中有些程式軟體還是沒辦法達到消費者的要求，例如：很多手機防毒軟體的程式都是內建的，無法自己設定，照自己的需求，如果研發團體把這些概念加入進去後，那想必應該會更符合更多消費者的需求，就讓手機防毒軟體變得更實用。

(二)本研究以樹德家商高中職生為範圍隨機發放問卷，故研究結果可能有無法類推至所有年齡層的部分，所以建議未來研究者，可以將研究範圍擴大，以求研究更精確。

肆●引註資料

1. CTIMES(2010)，挑戰與商機：手機資訊安全的前景，擷取日期：2013 年 11 月 05 日，網站來源：
   http://www.ctimes.com.tw/news/ShowCols.asp?O=201005051354131538
2. 張振浩(2010)，手機資訊安全拉警報，TrustZone 主動出擊新通訊，行家出手期刊 **9** 月號 **115** 期
3. 侯俊宇(2009)，手機安全議題不可忽視 安全驗證組織角色吃重新通訊，行家出手期刊 **6** 月號 **100** 期。
4. 張振浩**(**2010**)**：維護手機資訊安全 TrustZone 軟硬兼施新通訊，技術前瞻期刊 **10** 月號 **116** 期。
5. 張維君(2010)，Juniper 歡迎資安廠商加入開放平台 提供 API 強化行動應用安全，擷取日期：2013 年 12 月 05 日，網站來源：
   http://www.informationsecurity.com.tw/article/article_detail.aspx?aid=5955
6. 吳明蔚、江衍勳、林子群(2012**)**，資安防護整合服務委外服務案行動裝置資安防護，財團法人資訊工業策進會
7. 天下雜誌(2011)，機資訊安全最大問題在於人，擷取日期2013年12月04日。手機行動資訊安全要則，網站來源：
   http://www.inside.com.tw/2011/04/20/mobile-info-security
8. 吳傳輝(2011)，行動裝置當道 員工需有前瞻資安意識，擷取日期2013年12月14日。網站來源：
   http://www.netadmin.com.tw/article_content.aspx?sn=1112070001
9. 賴姿侑(2012)，行動社交網路攻擊變形再進化，以人為本才是防護重點，擷取日期2013年12月14日。網站來源：
   http://www.digitimes.com.tw/tw/dt/n/shwnws.asp?cnlid=13&cat=1&id=0000271008_FUPL8XYV1JZ4E17EF44J0&cat1=25&cat2=10