行動支付安全嗎？

■ 臺北市立中正高中資訊組長　李詩婷

107 年為臺灣行動支付元年，政府大力推動行動支付，民眾被行動支付的便利性所吸引，但也對其背後的安全風險有所疑慮，便利與安全應如何兼得？

行動支付時代來臨！

行動支付是政府近年來大力推動的國家發展政策之一，行政院賴院長於 106 年出席「行動支付購物節暨聯盟成立大會與聯合成果展」時，揭示於 114 年行動支付提升至 90% 的政策目標。行政院已將 107 年訂為臺灣行動支付元年，為了讓行動支付更為普及，相關部會陸續修訂與鬆綁法令，並推出眾多行動支付軟體，以建置友善的行動支付使用環境。政府大力推動行動支付，目的不僅在增加便民服務，亦希望藉此刺激消費、促進經濟成長。在政府及民間業者的努力下，行動支付使用率也逐年提升，根據金融監督管理委員會統計，截至 2018 年 4 月底，國內行動支付總交易金額已超過 281 億元，較去年同期成長 601%。

行政院賴院長出席行動支付購物節暨聯盟成立大會與聯合成果展，期望未來在政府與民間、業界的共同努力之下，行動支付產業能在 114 年如期達到普及率提升至 90% 的政策目標。（圖片來源：行政院，https://www.ey.gov.tw/Page/AF73D471993DF350/abb8f5b0-0c55-4760-a19b-a8761c7ae2df）

什麼是行動支付

行動支付簡單來說就是可利用行動載具（如手機）以非現金方式進行付款交易。交易方式主要又可分為兩種，一種是使用 NFC 功能進行感應刷卡，以國際三大 Pay（Apple Pay、

Google Pay 及 Samsung Pay）為代表，其特色是交易時是利用行動裝置內建的 NFC（Near Field Communication，近場通訊）功能進行感應傳輸，故不需要啟用網路，行動裝置充其量只是信用卡的載體而已。

另一種則是透過 QR Code 掃描方式進行支付，交易時需啟用網路，但因不限定廠牌手機與 NFC 通訊功能，進入門檻較低，故配合的商家最廣，如夜市或手搖茶飲店常見的街口支付或 Line Pay 等。

資安問題仍是民眾最大疑慮

民眾被行動支付的便利性所吸引，但也對其背後的安全風險產生疑慮。有據於此，金融監督管理委員會於 106 年修正了《電子支付機構資訊系統標準及安全控管作業基準辦法》，而中華民國銀行商業同業公會全國聯合會亦修正「信用卡業務機構辦理手機信用卡業務安全控管作業基準」等法規，目的就是在建立相關安全控制基準，規範支付平臺應具備完善之安全防護機制，以維護使用者個人資料安全。

行動支付交易方式一種是使用 NFC 功能進行感應刷卡，另一種是透過 QR Code 掃描方式進行支付。

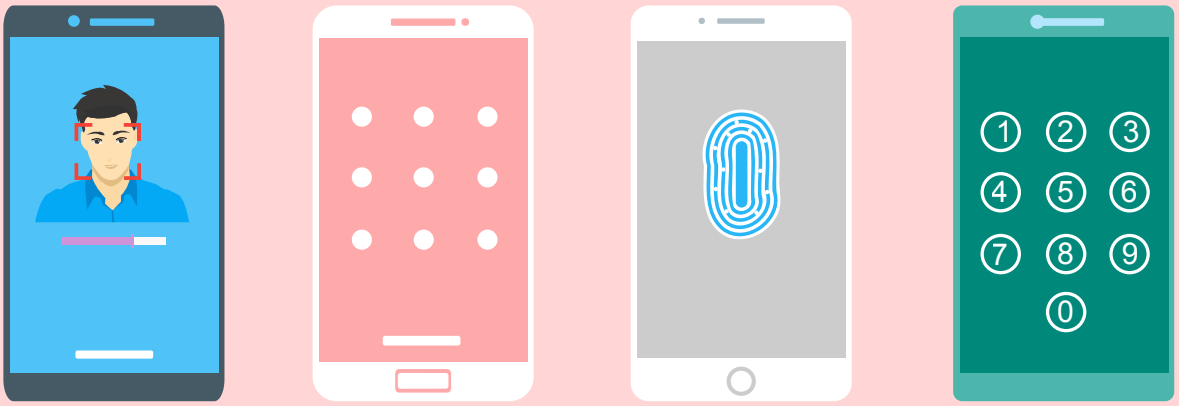
另外，針對行動裝置 APP 的安全問題，經濟部工業局已修訂「行動應用 APP 基本資安規範 V1.2」等相關文件，並新增「行動應用 APP 安全開發指引 V1.0」，提供行動支付商家在開發及檢測 APP 時作為參考依據，以加強資安防護。

相關業者及開發商為符合法令規範及維護自身商譽，亦須設計相關安全防護機制以降低資安風險，在不危及使用便利性下努力提高支付機制的安全性。舉例而言，Apple Pay 為了提高安全性，凡是設定使用 Apple Pay 的手機皆強制啟用螢幕鎖，並可搭配指紋辨識或 Face ID 以兼顧使用便利性。Google Pay 亦須設定螢幕鎖控制，不論是密碼、圖形或指紋皆可，且一旦移除螢幕鎖設定，裝置內綁定的信用卡設定也會一併移除。

使用者應具備基本資安意識

然而，行動支付最大的安全隱憂仍來自使用者的行動裝置使用習慣。手機螢幕鎖定方式一般包含圖形、密碼、及滑動解鎖等，若未開啟螢幕鎖定，或是解鎖密碼太簡單（例如使用慣用密碼 0000、1234、生日等）就容易被破解而盜用，使用圖形解鎖也須避免被旁人偷看或利用螢幕殘留的指紋痕跡進行猜測破解。當手機變成行動支付的載具，其效力就等同信用卡般重要，但**一般民眾不會將信用卡輕易離身，卻可能會將手機隨意置於座位後短暫離開，增加行動支付被盜用風險**。

多數行動支付 APP 依賴的是內建的密碼認證機制，而非手機密碼，例如街口支付、Line Pay 及台灣 Pay 等，於交易前必須



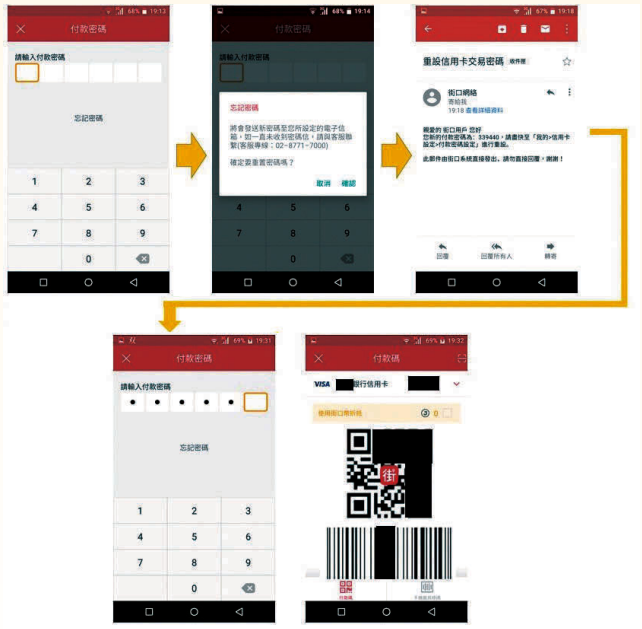
手機螢幕鎖定方式包含臉部辨識、圖形、指紋、密碼等，但都有被破解的可能，因此當手機變成行動支付的載具後，最好手機不離身，才能降低手機被盜用的風險。

輸入密碼後始能開啟支付功能，故並不會強制使用者啟用螢幕鎖控制機制。然而使用者仍需留意其內建的安全機制是否確實有效，即使在手機遺失時仍能及時發揮保護作用。建議使用者仍應以縱深防禦（Defense in depth）之概念，仍應啟用手機螢幕鎖定密碼。

以下以街口支付使用案例，說明縱深防禦觀念之重要性：

1. 小明拾獲小花的手機，發現小花未設定螢幕鎖定密碼，故小明可直接操作手機，並啟用街口支付 APP 欲進行交易付款。當使用「出示付款碼」功能時，APP 要求輸入付款密碼。
2. 小明點選「忘記密碼」功能，街口支付 APP 會發送暫時密碼至原使用者申請信箱。
3. 小明開啟手機的 Gmail，發現原使用者恰巧是以 Gmail 申請街口支付服務，故直接可檢視到系統所寄發的密碼通知信。
4. 小明取得新密碼後即可正常產生付款碼進行交易。

由以上案例可發現，小花因未設定螢幕鎖定密碼，且使用慣用的 Gmail 信箱申請行動支付服務，造成一旦手機遺失就會讓行動支付內建的密碼功能形同虛設。

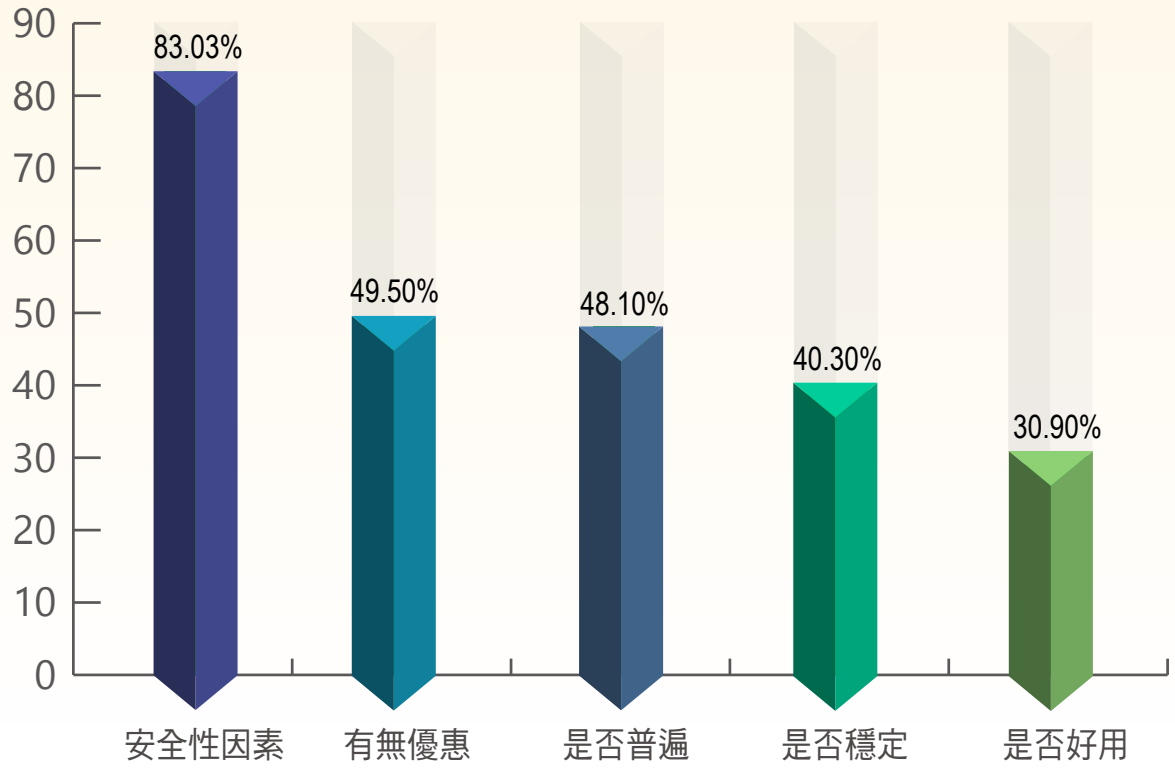


密碼驗證案例分析—街口支付。（圖片來源：作者提供）

結論

根據資策會產業情報研究所（MIC）在 2017 年 2 月所進行的「行動支付消費者調查分析」調查顯示，國人考量是否使用行動支付的前五名因素之中，安全性因素（83.3%）位居榜首，「有無優惠（49.5%）」則屈居第二，表示國人對行動支付的安全性疑慮比「優惠小確幸」更為看重。

是否使用行動支付的前五名因素



（資料來源：MIC 產業情報研究所；表格資訊：作者整理）

政府若欲達到行動支付普及率 90% 的目標，首先就要設法降低民眾對行動支付安全性的疑慮；然而，安全性是環環相扣的，在政府及業者努力提升行動支付機制安全性的同時，使用者亦應被教育培養資安意識，以養成正確的行動裝置使用習慣，避免成為整體安全機制內的最弱環節。

資安專家建議民眾應：

- 行動裝置啟用螢幕鎖定機制，強化資安縱深防禦。
- 避免下載來路不明的 APP 軟體，並安裝防毒軟體。
- 避免使用簡易密碼並時常更換。
- 小心保管行動裝置，若不慎遺失則可利用 Android 的「找回手機」，或是 Apple 的「尋找我的 iPhone」功能，定位手機位置或近一步進行裝置鎖定、資料清除等動作。

網路沒有距離，也沒有秘密

■ 陳鈺津

科技發展日新月異，短短幾年內大幅改變你我的日常生活，以前如同科幻電影中天馬行空的想像—智慧化的手機及家電，已逐漸成為我們生活中不可或缺的元素。

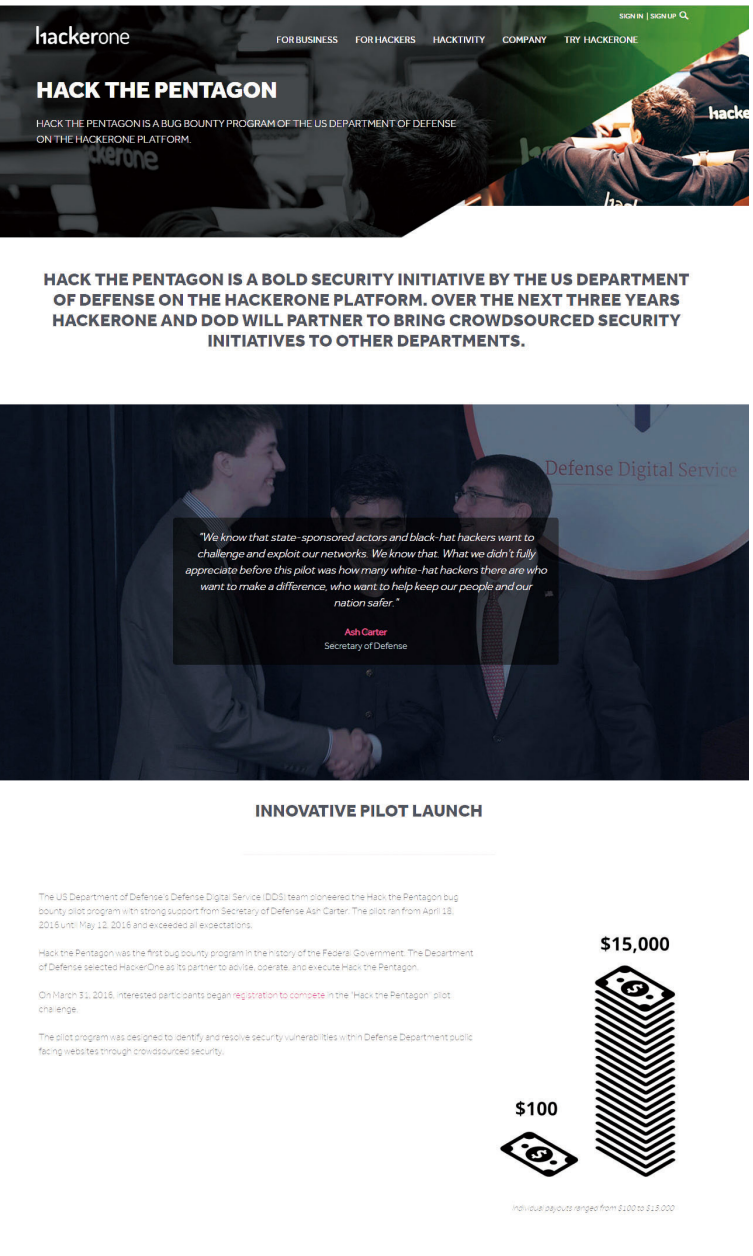
依據研究資料預測，到 2020 年全球將會有五百億筆資料在網際網路中流通，並透過網路空間交換、取得及蒐集等。也就是說，眾多機敏資訊在轉瞬間，便流傳於網路空間，無形中增大被滲透破壞與情蒐空間，不但極易肇生資訊安全危機，更將損及國家安全與利益。科技帶來生活上的便利，也同時伴隨潛在的問題，這些設備功能越是強大，我們對科技的依賴性越重，一旦遭到有心人士惡意破壞，所造成的傷害也越大。

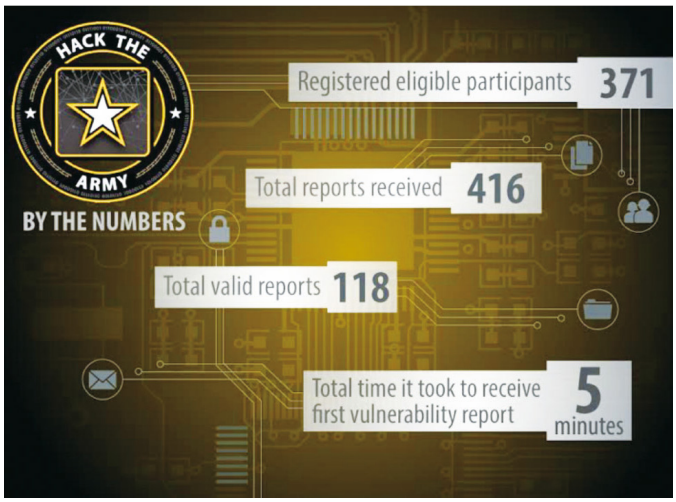
美國 2013 年《華盛頓郵報》曾報導，大批駭客企圖入侵美國國防部、國務院、能源部、國土安全部，甚至武器承造商的網路，並成功入侵眾多民間公司企業的網路；當時駭客隨意進出電腦系統，既沒有犯下鍵盤輸入上的錯誤，也沒有留下入侵途徑，過程僅僅不到 30 分鐘。美國國防部事後即意識到問題的嚴重性，並於 2016 年實施「駭入五角大廈」（Hack the Pentagon）計畫（之後陸續舉辦「駭入軍

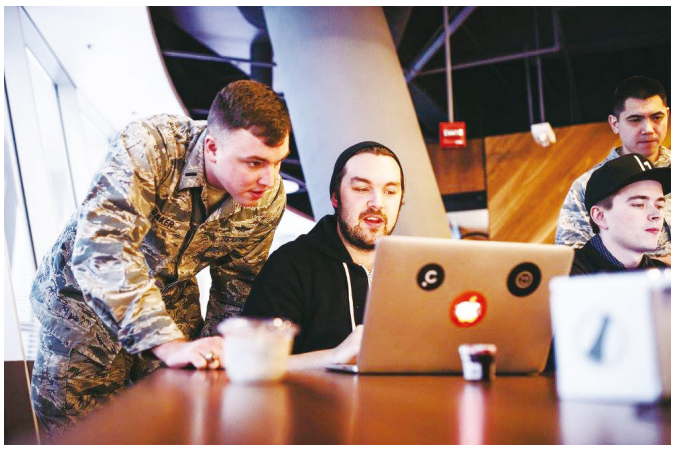
智慧化手機及家電為人們提供便捷的生活，但在日益依賴網路科技的同時，卻也可能衍生出不少潛藏的資安危機，造成國家安全與社會利益的損失。

隊 Hack the Army」及「駭入空軍 Hack the Air Force」等計畫），自實行迄今（2018）年，已藉由外部人員找出美國國防部等網站超過三千個以上的漏洞，美國因此頒發了逾廿七萬美元的漏洞獎金。此種僱用大批駭客，邀請他們測試及入侵官方電腦的方式，有助於美國國防部對症下藥，防患資安危機於未然。

市面上充斥著各式各樣的科技產品及五花八門的 APP，但其中隱藏許多資安漏洞與後門程式，往往在一時疏忽下，輕







美國國防部交由 HackerOne 承辦營運的 bug 賞金計畫「Hack the Pentagon」，此後更續推出「Hack the Army」、「Hack the Air Force」計畫，已為美國國防部等網站找出三千個以上的安全漏洞。（Photo Credit: HackerOne, https://www.hackerone.com; Official United States Air Force Website, https://www.af.mil/News/Photos/igphoto/2001855476/mediaid/2397030）

易將個人資料外流，因此，在使用產品或軟體時，應更加謹慎小心。現今由中國大陸設計、研製的部分行動裝置，因價格低廉、功能完善，吸引不少民眾青睞。但早在 2012 年美國眾議院提出的調查報告中，即指出部分中共廠商背後所隱藏的軍方背景，並已引起國安及商業機密遭竊疑慮。美國國防部更於今年 5 月初下令禁止全球的美軍軍事基地內零售商店銷售由華為和中興通訊製造的智慧型手機。

美國前資安長達布斯基（Lance Dubsky）於 2016 臺灣資訊安全大會上公開表示「臺灣是全球被網路攻擊最多的地區」；另依據微軟 2018 年亞太資安研究報告指出「臺灣 2017 年總計因資安威脅造成 270 億美金的經濟損失，將近臺灣 GDP 的 5%」。

面對資安威脅所造成之經濟巨大損失及國安風險，各機關除應持續落實「實體隔離」，建置嚴密的資安防護機制外，更應加強教育所屬建立正確保密觀念。使用各項科技產品時，應體認「網路上沒有距離，也沒有秘密」，公務機關更應避免透過社群媒體、通訊軟體談論機敏公務或傳輸資料，以免國家機密資料遭竊取。

全民若能有健全的保密認知，慎選資訊產品，便能在享受便利的同時，大幅降低資安威脅的風險。唯有每個人具備高度警覺的資安意識，個人隱私、企業利益及國家安全方能永保無虞。

美國前資安長 Lance Dubsky 來臺參加 2016 臺灣資訊安全大會時指出，臺灣是全球被網路攻擊最多的地區。（Photo Credit: Lance Dubsky's twitter, https://twitter.com/CyberCondor/status/706693272769576960）