論述 》管理 · 資訊

手機安全停看聽

智慧型手機越做越輕巧，功能卻越來越強大，人手一機時時低頭滑手機，上網、聊天、購物、轉帳、下單全靠它，我們天天享受它所帶來的便利，是否曾留意伴之而來的風險？手機詐騙事件時有所聞，要怎麼做才能保護自己與親朋好友？本文將提供幾點使用手機趨吉避凶之道跟大家分享。

賴柏宇（行政院主計總處主計資訊處分析師）

壹、前言

根據國際研究暨顧問機構 Gartner 的報告，2016 年個人電腦（PC）、筆記型電腦（NB）、平板電腦與行動電話的全球總出貨量約在 23 億台，而其中智慧型手機出貨量約 15 億台，反觀傳統 PC（包含桌上型和筆記型電腦）則一路下滑至 2.19 億台。時至今日，智慧型手機已大大的改變我們的生活型態，舉凡食、衣、住、行、育、樂等各方面，我們都對智慧型手機倚重甚深；除了生活大小事，在工作上，可能也把一些作業從傳統 PC 移往平板電腦或智慧型手機（例如電子會議、教育訓練等應用）。既然智慧型手機如此深入我們的生活中，那大家是否曾留意它的風險及安全性呢？例如手機可授與 APP（手機應用程式）許多種權限（如讀取檔案、刪除檔案、讀取電話簿聯絡人、…），大家在安裝 APP 時，是否曾留意這個 APP 會用到哪些權限？這些權限要求是否合理？以下簡要提供幾點注意事項跟大家分享。

貳、注意事項停看聽

一、手機基本安全防護

關於安全防護的議題，有個滿基本也滿現實的想法，就是人都有怕麻煩的心態，有心人通常也會找尋容易下手的目標，所以只要讓人覺得我們不

是那麼好下手，相對上就比較安全。而智慧型手機（及平板電腦）的防護，「螢幕鎖定」功能可說是最基本、也最簡單且有效的防護措施，通常手機都已內建此功能，一般無需另外安裝，建議大家啓用這項功能。這項基本防護措施可以避免他人對手機的不當操作：如窺探隱私、竄改設定、安裝惡意軟體、…等，常見的螢幕鎖定解除方式有密碼、圖形、指紋、臉型辨識等，使用上選擇慣用的方式即可。要提醒的是，若是選擇用密碼保護，建議不要太短也不要用生日這種容易猜的號碼，另外，進入待機的閒置時間建議不要太久，比較安全兼可節省電力（圖1）。

圖 1　螢幕鎖定是最基本、也最簡單且有效的防護措施

資料來源：手機螢幕截圖。

二、只從官方商店安裝 APP

智慧型手機強大之處，即在於它可以安裝各式各樣的APP，提供各種便利的服務。而不同的手機系統，無論是蘋果（iOS）或安卓（Android），安裝 APP 都需透過商店（App Store、Google play）安裝，雖然也有不透過商店安裝的方式，但比較不建議使用。暫且不論商店是否會把關 APP 之安全性，至少商店是一個公開場合，登載很多資訊供大家參考，如功能說明、開發人員、下載數、評價、所需權限等，大家可在參考這些資訊之後挑選合適的 APP 來安裝，相對來說會比下載來路不明的 APP 要安全許多。

三、最小權限原則

此外，即便是從商店安裝 APP，我們也要留意其所需之權限。在安全防護上有個概念是「最小權限原則」，這是說欲達成某個目的，應賦予其所需最少權限，而非濫給過大的權限。舉大家普遍都有安裝的「手電筒」APP 爲例，要使手機發光的基本權限僅需「相機」、「控制閃光燈」即可，若有一款手電筒 APP，要求「修改或刪除 USB 儲存裝置的內容」、「裝置 ID 和通話資訊」、「完整網路存取權」等權限，那我們就要思考，爲何這個手電筒 APP 需要這些權限？雖然不見得這樣的 APP 一

論述 》管理 · 資訊

定有問題，但過多的權限要求確實會提高手機受到錯誤（或惡意）行爲破壞的風險，建議大家安裝 APP 時還需多加確認權限之必要性。安卓的做法在 Android 5.9 版之前，是安裝前可在商店確認 APP 的權限，如不接受就不安裝；到了 Android 6.0 之後的版本就跟蘋果（iOS）的做法類似，是安裝後才進行權限的確認（圖 2）。

四、不點選來路不明的簡訊、連結

現在的智慧型手機，除了可接收傳統簡訊，大家多多少少也都安裝了通訊軟體（如 LINE、Juiker 揪科）、社群軟體（如 FB）、eMAIL，在以往，詐騙集團或有心人士會利用傳統簡訊傳送惡意內容，而現在多移往通訊軟體，一來通訊軟體幾乎都是免費使用無需成本，再者通訊軟體提供五花八門的貼圖，吸引大家使用。由於大家愛用，所以通訊軟體也變成許多惡意簡訊的溫床，這類手法的對付方式也很簡單，跟對付釣魚信件的防範方法相似，就是保持警覺，不要隨意點選來路不明的簡訊、連結。

圖 2　安裝或使用 APP 前，務必確認該 APP 所需之權限

資料來源：https://play.google.com。

五、確認訊息來源

這邊特別跟大家分享另一種手法，跟惡意簡訊很類似，但危險性卻大大增加，就是假冒熟人法。筆者就曾有這樣的經驗，在以前 MSN 流行時，曾被朋友傳訊要求代買線上遊戲點數（可變賣或兌換回金錢），由於訊息是由朋友傳來而非來自於陌生人，當下的心境確實比較放鬆而無警覺性，幸好那位朋友平時不玩遊戲，跟他確認後知道是別人冒用他的名義進行詐騙，這詐騙手法才沒得逞。MSN 雖已像是遙遠的過去，不過相似的手法仍在通訊軟體、社群軟體上大行其道，例如最近的新聞揭露，有詐騙集團冒用親友身分來詐取 LINE 的驗證碼，企圖入侵 LINE，一旦被入侵成功，本身將淪爲被冒用身分的對象。平時用 LINE、Facebook 跟朋

友聯繫雖然很方便，不過討論的事項如果比較敏感（例如涉及金錢、個資、隱私、驗證碼、…），建議還是以電話或當面聯繫。

六、安裝個防護 APP

考量到手機功能越來越強大，建議還是幫手機安裝個防護 APP 吧。爲何要稱爲「防護」軟體而不稱「防毒」軟體呢？因這類軟體不只做基本的防毒（惡意程式），還需包含防止安裝有害 APP、防止隱私洩漏、來電與簡訊辨識、網站安全瀏覽、甚至是防盜等功能，這類防護軟體都有專業機構會進行評鑑，大家可參考權威評鑑（如 AV-Comparatives、AV-TEST）挑選適合自己手機的防護 APP（圖 3）。

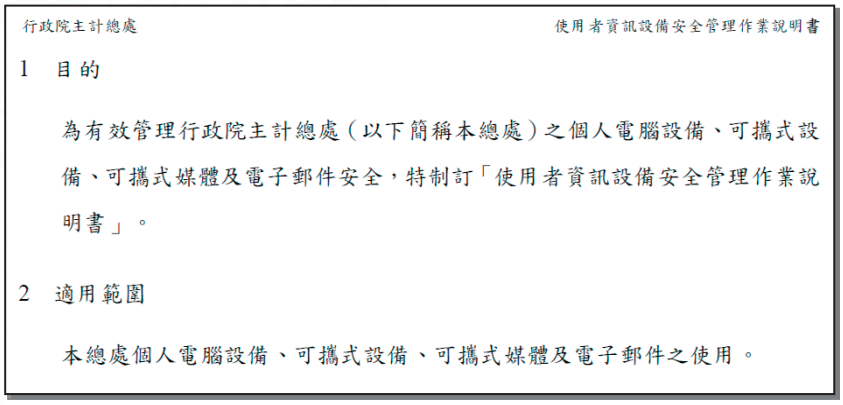
七、淺談組織應用行動裝置之注意事項

手機、平板等行動裝置集輕巧、便於攜帶、功能強大等好處於一身，若應用於公事上，對於提昇工作效率應有正向幫助。惟組織若有意導入行動裝置應用於公事上，宜先審慎考量其風險，制訂相關管理規範後才施行，而非貿然開放使用。組織會面臨哪些風險呢？試思考以下幾點：組織只允許員工使用配發的行動裝置處理公事，或是也允許使用私人手機處理公事？若只允許使用配發的行動裝置，有多少預算可供採購相關設備及管理系統？會否因預算不足而採購了不夠安全的設備？若開放使用私人手機處理公事，如何管控個人使用之 APP 以避免危害或洩漏組織資料？除此之外，尚有身分認證、資料傳輸、設備遺失、隱私保護等林林總總之風險議題。建議組織先釐清行動裝置於公事應用上之領域、範圍，掌握需要保護之資產，才能限縮風險，以便制訂管理規範，以及相關之解決方案（下頁圖 4）。

圖 3　現在的手機防護 APP，除了基本防毒，還附加許多防護措施

資料來源：https://play.google.com。

圖 4　組織內使用行動裝置應先制訂相關管理規範



行政院主計總處　　使用者資訊設備安全管理作業說明書

1　目的

為有效管理行政院主計總處（以下簡稱本總處）之個人電腦設備、可攜式設備、可攜式媒體及電子郵件安全，特制訂「使用者資訊設備安全管理作業說明書」。

2　適用範圍

本總處個人電腦設備、可攜式設備、可攜式媒體及電子郵件之使用。

資料來源：行政院主計總處。

參、結語

科技日新月異，相應而生的惡意手法也層出不窮，智慧型手機大大便利我們的生活，改變了我們的習慣，也帶來新型態的風險。防範之心不可無，對於手機的使用應保持適度的警覺性，平時留意一些防護新知、或詐騙新聞報導，瞭解趨吉避凶之道，自可享受手機帶給我們的便利生活。

參考文獻

1.Gartner, Inc.，Gartner Forecasts Flat Worldwide Device Shipments Until 2018，http://www.gartner.com/newsroom/id/3560517

2. 行政院國家資通安全會報技術服務中心，行動裝置安全注意事項，http://www.nccst.nat.gov.tw/MobileSafetyTips

3. Google Play 說明，檢查應用程式權限（Android 5.9 版），https://support.google.com/googleplay/answer/6014972?hl=zh-Hant&ref_topic=6046245

4. Google Play 說明，管理應用程式權限（Android 6.0 以上版本），https://support.google.com/googleplay/answer/6270602?hl=zh-Hant&ref_topic=6046245

5. 警政署 165 反詐騙，https://www.165.gov.tw/

6. 安全達人｜資安趨勢，https://blog.trendmicro.com.tw/

7. 資安人，正視企業資安課題－五步驟檢測資安防護，http://www.informationsecurity.com.tw/article/article_detail.aspx?aid=8250 ❖