陽光月刊 112 年 12 月號
目錄

反賄選宣導


移民署
IMMIGRATION
廉政官
嚴查賄選
斷絕賭盤
阻絕境外勢力
檢舉獎金
最高 2,000萬 元
檢舉專線
0800-024-099*4
法務部
MINISTRY OF JUSTICE
反賄選 斷黑金
好友募集中
LINE@啄木鳥公民巢
i幸福行動聯盟
廣告

資訊安全維護宣導

行動應用程式資安威脅及防護

一、簡介

APP 是應用程式(Application)的縮寫，是一種軟體應用程式，主要是在智慧型手機或行動裝置中使用。

行動應用 APP 依其功能可區分為遊戲類、教育類、商業類、生活風格類、娛樂類，以及工具類等數種類型。

正因為行動應用 APP 的廣受歡迎，使得駭客逐漸將駭侵或病毒散佈的目標從電腦轉向行動裝置的 APP 上，並且藉由使用者對 APP 的信任，透過行動應用 APP 進行惡意行為，從而獲取不法利益。

二、行動應用資安威脅

(一)行動應用 APP 資安威脅分析

行動應用 APP 的資安威脅，統稱為惡意行動應用程式(Malicious Mobile Applications)，透過吸引使用者的某些功能或活動，誘使使用者下載並安裝該 APP，進而自動安裝惡意程式以竊取行動裝置中的資訊，甚至修改裝置內相關設定。

根據賽門鐵克 ISTR 報告，單純的惡意 APP 數量有逐漸下降之趨勢，然而勒索性的 APP 卻上升了，尤其是針對企業的勒索攻擊。因此，不論是企業或個人，對於行動裝置的安全防護，必須保持一定的警覺。

在所有的惡意 APP 中，比例最高的為工具類型，其次為生活風格類型，再其次為娛樂類型之 APP。工具類型的 APP 通常會要求給予較高的使用權限，駭客即利用此較高的授權，進行資料竊取、修改設定等惡意行為。

(二)行動應用 APP 資安威脅及案例

隨著 APP 數量以及使用者將機敏資訊存於行動裝置的比例增加，惡意 APP 對使用者的威脅以及損害程度逐漸上升。除了個人使用者外，企業同樣也遭受惡意 APP 的入侵，這些惡意 APP 可被分為以下五種類型：

1. 廣告(Adware)：經常偽裝成一般合法應用程式，並涉及購買行為。
   美國的移動安全防護及分析公司 Wandera，曾發現 Google Play 商店中的兩款美肌 APP 會跳出惡意廣告，並且加速行動裝置的電量流失。因此，當使用者下載行動應用 APP 後，若有廣告出現或是行動裝置的運行速度變慢，電池耗用增加，極可能是下載並遭到惡意 APP 的侵襲。
2. 網路釣魚(Phishing)：此種類型之惡意 APP 主要是將使用者導入釣魚網站，並且誘導使用者輸入相關資訊，以竊取個人資料。趨勢科技發現在 Google Play 商店中，有多款美肌相機 APP 會將使用者導入釣魚網站中並使其留下個資。因此，若使用者在下載並安裝行動應用 APP 後，突然收到關於贏得獎品，或帳號、訂閱服務將被停止等訊息，都極有可能遭到網路釣魚 APP 的駭侵。
3. 殭屍網路(Bots)：此種惡意 APP 可以在行動裝置後台運作，和殭屍控制主機(botmaster)聯繫並執行命令，使用者不易察覺。
   曾有一款名為 Hidden Administrator 的惡意 APP，以 Android 系統為目標，在進入受害者行動裝置之後便隱藏起來。此應用程式會將自己的權限提升至管理員等級，並且控制該受害行動裝置，使變成殭屍網路或挖礦的工具。因此，若使用者在下載並安裝 APP 後，其行動裝置容易產生連線中斷、網路無法連接，或是在未經使用者授權的情況下，行動裝置自動安裝或移除任何 APP，則該行動裝置極有可能已下載到殭屍惡意 APP。
4. 間諜軟體(Spyware)：會監控和記錄使用者的裝置狀態或行為資訊，例如簡訊、電子郵件、電話紀錄、聯絡人、地理位置等訊息，並分享給遠端的伺服器。
   趨勢科技發現六款於 Google Play 商店上架之間諜軟體 APP。這六款惡意 APP，都是由被稱為「MobSTSPY」的間諜軟體偽裝而成，當使用者啟動後，間諜軟體會檢查行動裝置的網路狀態，搜集裝置型號等設備資訊，以及簡訊、電話簿等使用者資訊，再將竊取的資訊回傳給中繼站伺服器。因此，使用者在下載並安裝行動應用 APP 後，若發現行動裝置有奇怪的行

為，除了應將可疑的 APP 移除外，也必須檢查內部是否有被安裝或放置可疑的檔案及程式，並將其移除和卸載。

5. 下載器(Downloader)：此種程式自身並非惡意程式，但會隱身於 APP 中，負責下載其他的惡意程式到使用者行動裝置中。
   以色列資安公司 Check Point，在 Google Play 商店中發現一款新的惡意 APP。該惡意 APP 具有開啟特定網址的功能，並進行網路釣魚行為，也能替受害行動裝置安裝新的惡意程式。因此，當使用者下載並安裝 APP 後，若出現未經使用者授權下載之 APP、檔案，或突增電池耗用、網路流量，以及額外費用等，都可能是行動裝置遭惡意下載器感染所致。

三、行動應用防護

(一)行動應用 APP 防護機制

惡意 APP 難以完全防範，使用者在下載行動應用 APP 之前，必須注意下述幾點：

1. 定期更新行動裝置作業系統或應用程式之版本，配合廠商進行漏洞修補，提升防護能量。
2. 僅從信用良好的應用程式商店下載行動應用 APP。
3. 許多惡意 APP 會偽冒知名品牌或企業的標章，下載前須檢查並識別該 APP 是否確為該品牌或企業所屬。
4. 在下載並安裝 APP 前，仔細閱讀其授權聲明，避免提供非該 APP 所必需的授權，以免洩漏行動裝置中的機敏資料。
5. 使用者可以安裝行動安全應用程式，協助辨識惡意 APP，以隔絕並保護行動裝置中的機敏資料。
6. 為了減少行動裝置或資料因惡意 APP 遭到破壞，建議使用者定期備份手機中的機敏或重要資訊。

美國的 Web 應用安全非營利組織 OWASP，提出了開發行動應用 APP，必須注意並避免的 10 個安全項目 Mobile Top 10：

1. 平臺使用不妥當(Improper Platform Usage)：主要為開發者未確實使用平臺權限、TouchID 等安全控管機制。為了防止平臺使用不當，在行動應用 APP 開發時，必須在伺服器端實踐安全編碼(Secure Coding)及安全相關設置。
2. 不安全的數據存取(Insecure Data Storage)：當開發者未針對文件或機敏資訊的存取進行管控時，就容易出現存取漏洞。因此，開發者必須避免使用較差的加密資料庫，並應設定須透過特殊的工具方能進行數據存取。
3. 不安全的通訊(Insecure Communication)：在行動應用 APP 數據傳輸的過程中，駭客可以透過系統或設備的漏洞竊取傳輸中的機敏資料。因此，開發者必須注意資訊傳輸的安全設定，或使用可信的憑證中心所提供的簽章，防止因通訊不安全造成的損失。
4. 不安全的身分驗證(Insecure Authentication)：由於行動裝置經常只要求使用者輸入短密碼，導致易於被破解入侵。因此，開發者必須避免較弱的身分驗證模式，確保相關程序都在通過嚴謹身分驗證後方可使用。
5. 不足夠的加密法(Insufficient Cryptography)：若開發者未使用足夠且有效的加密法，則駭客容易入侵竊取資料，甚至還原加密數據。因此，開發者應使用經過驗證且經得起考驗的加密標準，替相關資訊加密。
6. 不安全的授權(Insecure Authorization)：若開發者使用較為脆弱的授權方式，則駭客可能會以合法使用者的身分登入 APP 中，取得其不應取得的權限。因此，建議開發者應使用後端伺服器中的訊息進行驗證，避免使用來自於行動裝置的權限資訊進行授權驗證。
7. 較差的程式碼品質(Poor Code Quality)：此種類型的問題，本身並不一定是安全問題，但容易引發安全的漏洞。因此，開發者必須確保在開發團隊中，都維持一致的編碼方式。
8. 程式碼竄改(Code Tampering)：由於 APP 及大部分數據都置於行動裝置中，駭客可能入侵後竄改 APP 中的程式碼，或是更動記憶體中資訊等。因此，開發者必須提供驗證機制，檢測該行動應用 APP 是否曾經遭到他人竄改，並執行適當處置行為。
9. 逆向工程(Reverse Engineering)：駭客可能透過某些工具針對 APP 進行反組譯解析，或是從中得到該 APP 的相關資訊、機敏資料等，甚至藉以對

後端系統進行攻擊。因此，為了防範逆向工程，開發者必須使用混淆工具，將其程式碼、字符表等資料進行混淆處理，避免輕易遭到逆向工程的威脅。

10. 額外功能(Extraneous Functionality)：許多開發者為了方便進行程式的修改或安全控管，會在 APP 的程式碼中留下額外功能，雖不具惡意，但卻可能被駭客利用來入侵並竊取相關資訊。因此，為了防範此資安問題的發生，通常須由資安專家對該行動應用 APP 進行程式碼檢查，方能確保沒有任何隱藏功能。

數位發展部也邀集國內資安領域專家，參考國內外檢測標準，提出行動應用 APP 基本資安規範，分別從「行動應用程式發布安全」、「安全敏感性資料保護」、「交易資源控管安全」、「行動應用程式使用者身分鑑別及授權與連線管理安全」、「行動應用程式碼安全」及「伺服器端安全檢測」等六個層面提出資訊安全技術要求，供業界開發行動應用程式時依循參考，以提高行動應用 APP 的安全品質。

另為提供第三方機構針對行動應用程式，進行資訊安全檢測及評估其安全水準之依據，進而發布「行動應用 App 基本資安檢測基準」，以行動應用程式之功能分類，訂定各類別之安全要求範圍，分為三級：

L1：無須使用者身分鑑別之行動應用程式。

L2：須使用者身分鑑別之行動應用程式。

L3：含有交易行為之行動應用程式。

欲進行檢驗之行動應用 APP，若同時符合兩個以上之類型特徵，則以符合類型中檢測項目較多者做為檢驗依據。

(二)行動應用 APP 安全檢測概況

根據行動應用資安聯盟的數據，在總體通過驗證之 APP 中，通過的行業類別佔比分別為：金融業 57.2%、其他類別(如工具類)34.4%、醫療 4.7%、行動支付類 2.1%、通訊類 1.6%。

再針對三個檢測基準進行統計，在總體通過驗證之 APP 中，通過 L1 級佔比 8%、L2 級佔比 36.6%、L3 級佔 55.4%。

四、分析與建議

1. 行動應用 APP 隨著行動裝置的普及正快速成長，將是未來軟體發展的一大重點。
2. 隨著行動應用 APP 的普及，其相關之惡意程式也逐漸增多，且因為企業允許個人自備裝置(BYOD)數量的增加，以致惡意行動應用程式對企業的威脅也逐漸上升。
3. 行動裝置中勒索惡意 APP 的數量有上升趨勢，代表駭客將許多勒索軟體從電腦轉而以行動裝置做為目標。
4. 台灣因惡意 APP 受害的比例略高於全球平均，因此使用者仍須注意行動應用 APP 的使用，避免遭受惡意 APP 的攻擊。
5. 為減少惡意 APP 之威脅，使用者宜定期更新行動裝置作業系統、相關軟體及應用程式，盡量從信用良好之應用程式商店下載 APP，並識別商標、檢驗其功能權限。也應定期備份裝置中的重要資料或機敏資訊，以降低損害風險。
6. 美國的 Web 應用安全非營利組織 OWASP，提出了開發行動應用 APP 最可能發生的 10 個弱點，希望開發者能在進行 APP 開發製作時加以注意，以減少資安漏洞，達到較佳的 APP 資安防護。
7. 我國政府也針對行動應用程式的開發，發布「行動應用 APP 基本資安規範」，以及「行動應用 App 基本資安檢測基準」，提供 L1、L2、L3 三個等級對應需檢測驗證的項目，以提高 APP 的資訊安全。
8. 由於行動應用 APP 隨著行動裝置的蓬勃發展，其數量逐年快速增加，許多病毒或駭侵手法也從電腦轉往行動裝置。除了使用者需注意並維持行動裝置的安全外，開發者更應針對所開發之行動應用 APP 進行全面檢測，建議可尋求相關資安檢測實驗室協助驗證，以提高其安全性，並讓使用者放心使用。

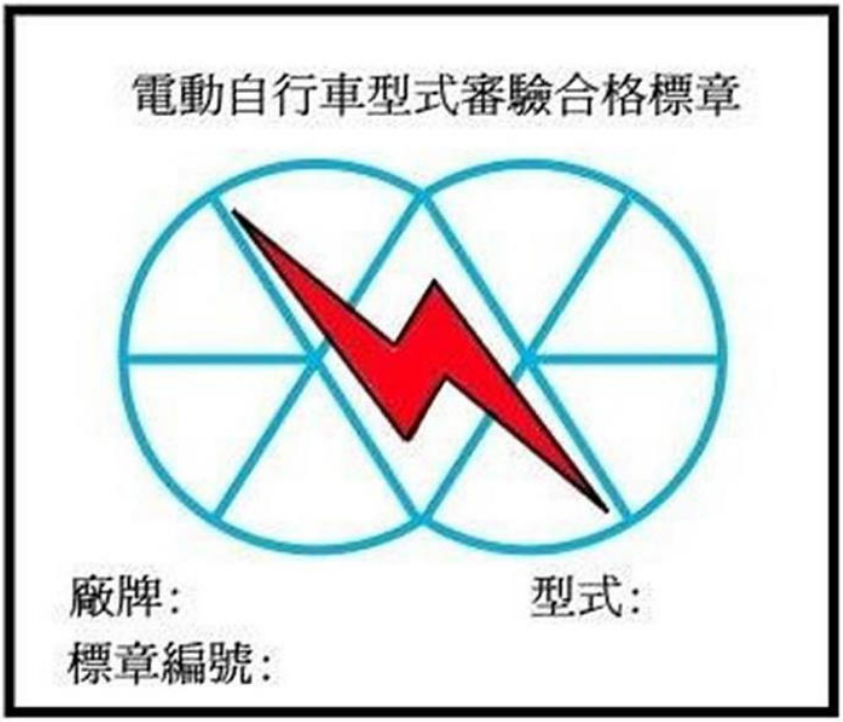
以上內容轉載自 TWCERT/CC 台灣電腦網路危機處理暨協調中心網站

發布單位:TWCERT/CC。更新日期:2023-02-06

安全維護宣導

電動自行車請勿擅自改裝，以免引火上身！

彰化縣北斗鎮 10 月份發生 2 件充電中電動自行車火災，均為外籍移工使用，因 2 案起火車輛皆停放於工廠內部停車區，共波及 20 餘輛電動自行車燒損，經消防局調查發現，起火車輛車體及電池動力系統經過使用人自行改裝，研判起火原因為充電系統發生過充短路引起火災，鑑此，呼籲電動自行車車主勿擅自改裝，尤其是換裝來歷不明鋰電池或增改電子控制系統，將大幅提高電動自行車火災風險。



合格標章(紅色閃電)©由 CNA 提供

據統計台灣外籍移工數逐年遞增，電動自行車因價廉、輕巧方便，機動性高，加上不需駕照便可騎乘，近年來已成為外籍移工代步交通工具首選，電動自行車需求隨之增加，但受限於道路交通管理處罰條例規定，微型電動二輪車最大行駛速率每小時二十五公里以下，因此有不肖業者看準使用者有提升時速的需求，於

網路販售改裝鋰電池，或私下提供改裝控制裝置解除速率限制服務，藉以加大馬力提升行駛速率，此舉不但增加車輛故障機率，更可能造成火燒車意外。

經統計彰化縣 110~112 年已發生 24 起電動自行車火災事故，彰化縣消防局表示，品質不良鋰電池容易發生熱失控，過充、過放或碰撞都可能造成電池溫度升高起火燃燒，因此，購買電動自行車應選購經交通部型式審驗合格之產品，並嚴禁改裝，提醒民眾要防範電動自行車自燃起火，請謹記以下 5 點。

一、選購經交通部型式審驗合格商品，認明合格標章，電動自行車應有紅色閃電標識。

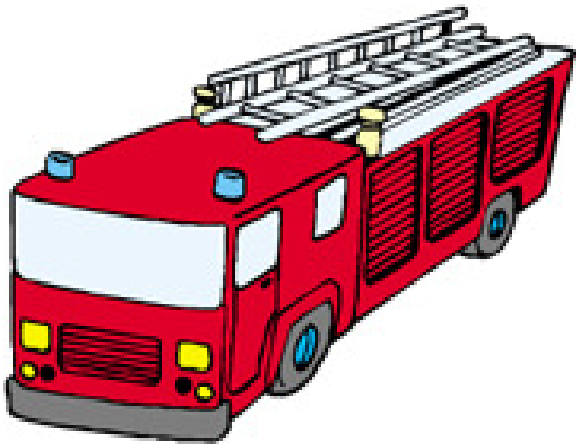
二、勿自行加裝、改裝鋰電池及電氣系統，若變更原廠配電設計，恐造成電力系統負載增加或不穩，提高接觸不良及電線短路起火風險。

三、電動自行車均有專屬充電器，不同型號充電器不可混用。

四、老舊車輛在長時間運轉使用下，車內電源端子接點及配線接續處可能因震動、拉扯、老化造成接觸不良或短路問題，當發現電池或電氣系統故障應立即檢修。

五、充電時應避開樓梯間、通道或出入口處，並與易燃物保持適當距離，避免造成延燒。

(以上內容轉載自中央通訊社網路新聞 20231107 09:28:50)



消費者訊息

以上內容轉載自行政院消費者保護會網站