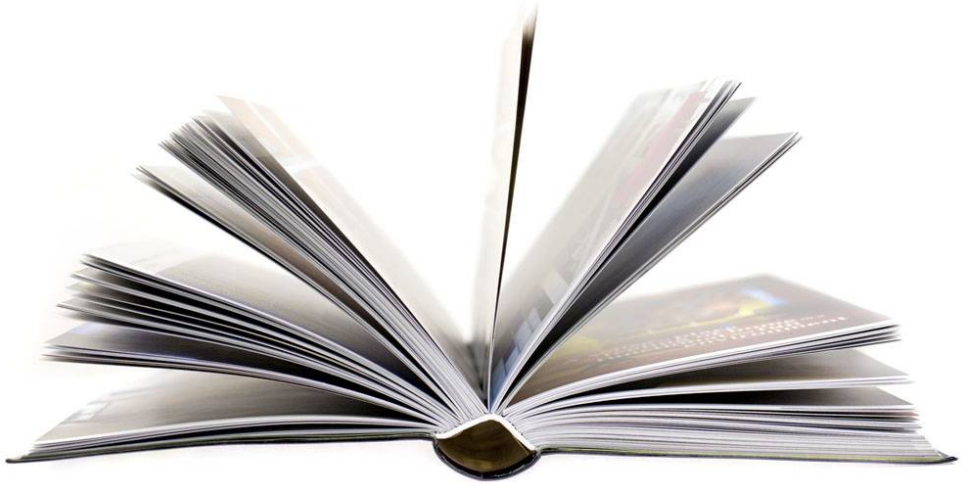
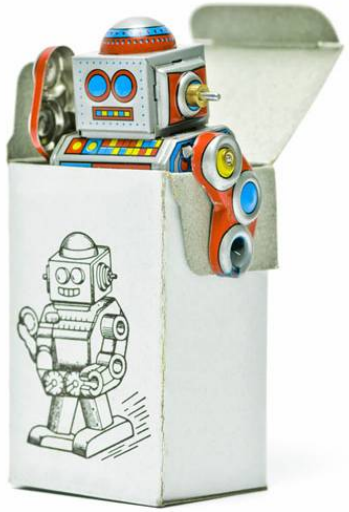
法務部調查局

法務部調查局
ISMS驗證複審顧問服務案
一般人員資安宣導教育訓練



簡報大綱

- 資安事件案例及資安觀念分享
  - » 您用的APP安全嗎？手機/行動裝置APP探討
  - » 雲端服務好方便？雲端服務潛藏風險探討
- 日常作業 vs. 資訊安全
- 動動腦時間

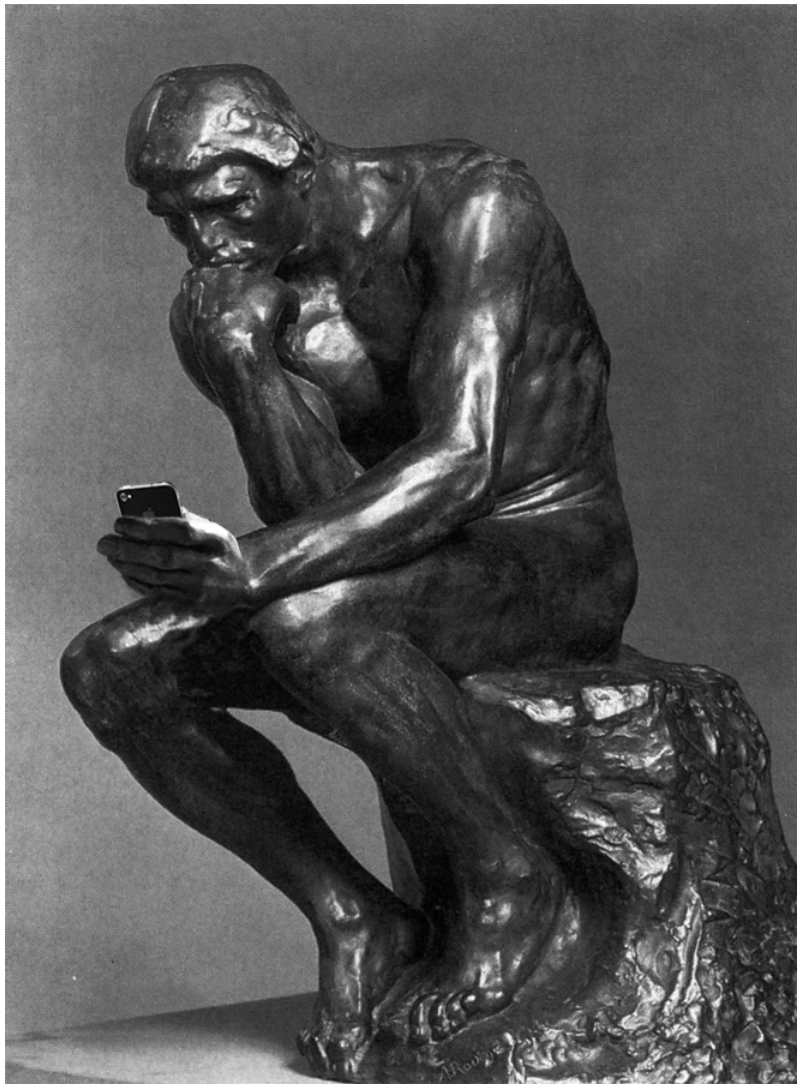


【資安事件案例及資安觀念分享】

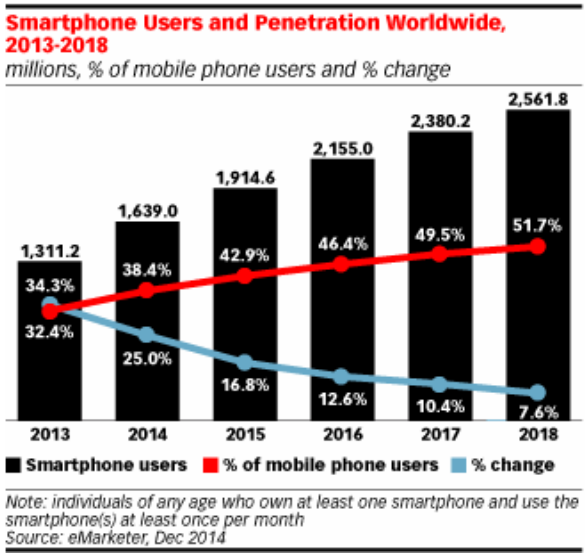
您用的APP安全嗎？

手機/行動裝置APP探討

您是低頭族嗎？



- ◆全球手機使用人數為45.5億
- ◆智慧型手機使用人數：
  - 2016年預估21.5億(42.9%)
  - 台灣1432萬人 (61%)
- ◆在 2020 年，將有 750 億件裝置與網路結合。



法務部調查局

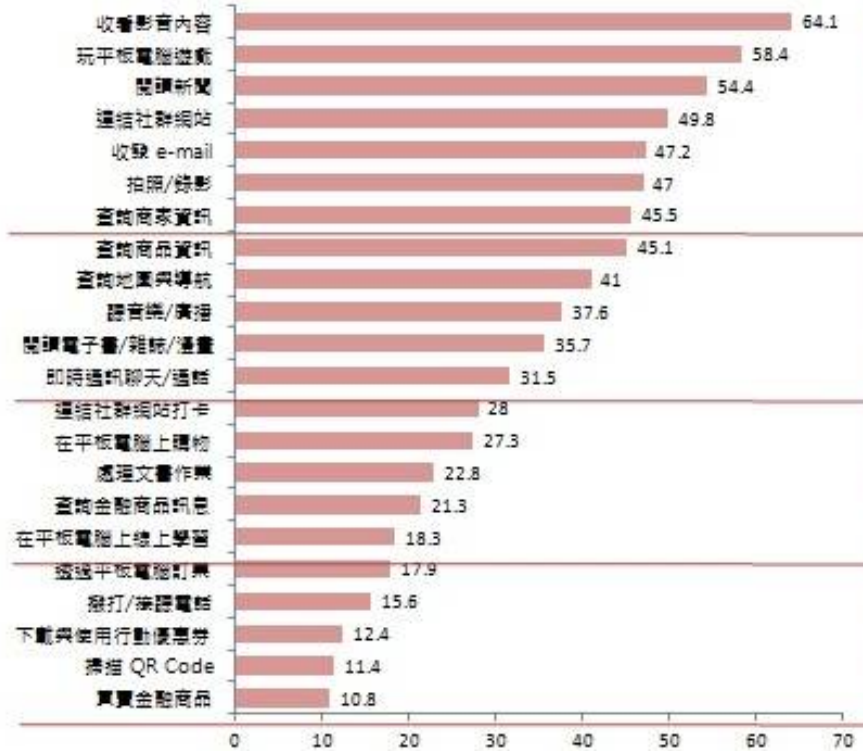
台灣人對手機依賴程度位居亞太之冠!

- Google在2013年公布了台灣人使用智慧型手機習慣的調查，發現台灣智慧手機的普及程度不但高達50%，勝過日本，還有超過八成的使用者出門一定會隨身攜帶手機。超過56%的台灣使用者每天花超過半小時使用手機，更有約22%的人超過2小時以上，相對於國外，美國人平均每天使用手機的時間則是58分鐘。調查更指出，超過93%台灣的使用者會透過手機連結社群網路，愛分享的頻率也位居亞洲第3，高達41%。

Google調查台灣用戶的手機使用習慣後發現，台灣人對手機的依賴程度位居「亞太之冠」。

您都怎麼用手機呢？(in台灣)

- 台灣人最常使用智慧型手機做的事情：
  - » 看影片、玩遊戲、看新聞、逛社群網站、收發email...等



男性	女性
(177)	(153)
63.6	64.5
59.3	57.2
56.6	51.9
55.6	43.1
54.8	38.4
45	49.3
48.6	41.9
46	44.1
43.5	38.2
42.4	32.1
40.6	30.1
32.4	30.4
30.1	25.6
26.6	28.2
23.8	21.7
24.2	18
18.4	18.2
17.3	18.7
12.7	19
14.3	10.1
13.9	8.5
13.1	8

資料來源：資策會FIND(2014H1)/經濟部技術處「服務創新體驗設計系統研究與推動計畫」
調查期間：2014.5.16-6.09；有效樣本：330份
Q.請問，您有經常使用平板電腦做以下哪些事情?

法務部調查局

您都怎麼用手機呢？(in美國)

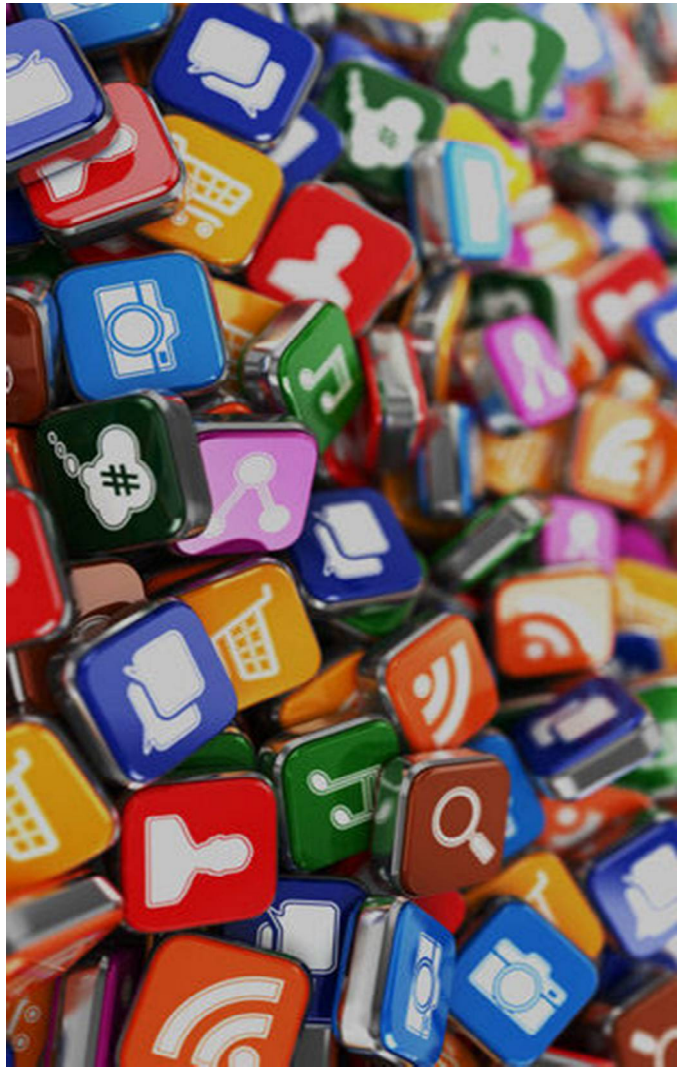
- 近六成的民眾，常從事搜尋健康資訊，及銀行相關活動（像是轉帳、交易）
- 近四成的民眾，會透過智慧型手機搜尋住處、找工作，或是搜尋政府相關資訊
- 三成的民眾，透過智慧型手機參加線上課程或教育
- 兩成的民眾，透過智慧型手機遞交職缺申請表

您曾使用手機辦公嗎？

根據Juniper Networks所發布一項全球性消費者調查報告，在16個國家、超過6,000名智慧型手機和平板電腦使用者當中...有高達81%的受訪者承認在雇主不知情或未獲允許的情況下，利用行動裝置存取公司網路，且有超過一半的人每天都這麼做；更值得注意的是，有超過76%的受訪者使用智慧型手機或平板電腦存取機密的個人或商業資訊。

您的手機裡有多少APP呢？ 來源？

- Google Play App數量143萬，Apple AppStore 121萬。
- 中國App數量 30 萬 (2013年底)
- 其他非透過App商城的下載管道(例如：.apk檔)
- 根據調查，國內iOS用戶平均下載32個，Android用戶平均下載17個App



手機中也有惡意程式！？

- 根據趨勢科技2014年調查，運行於手機上的惡意程式已經超過200萬個(2014/4)
- 趨勢科技預估2015年Android惡意程式會達到800萬個
- 根據McAfee的調查，高達1/6的App是具有風險的，其中8%包含惡意程式

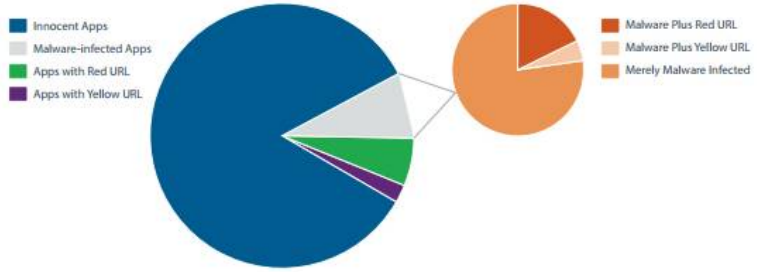


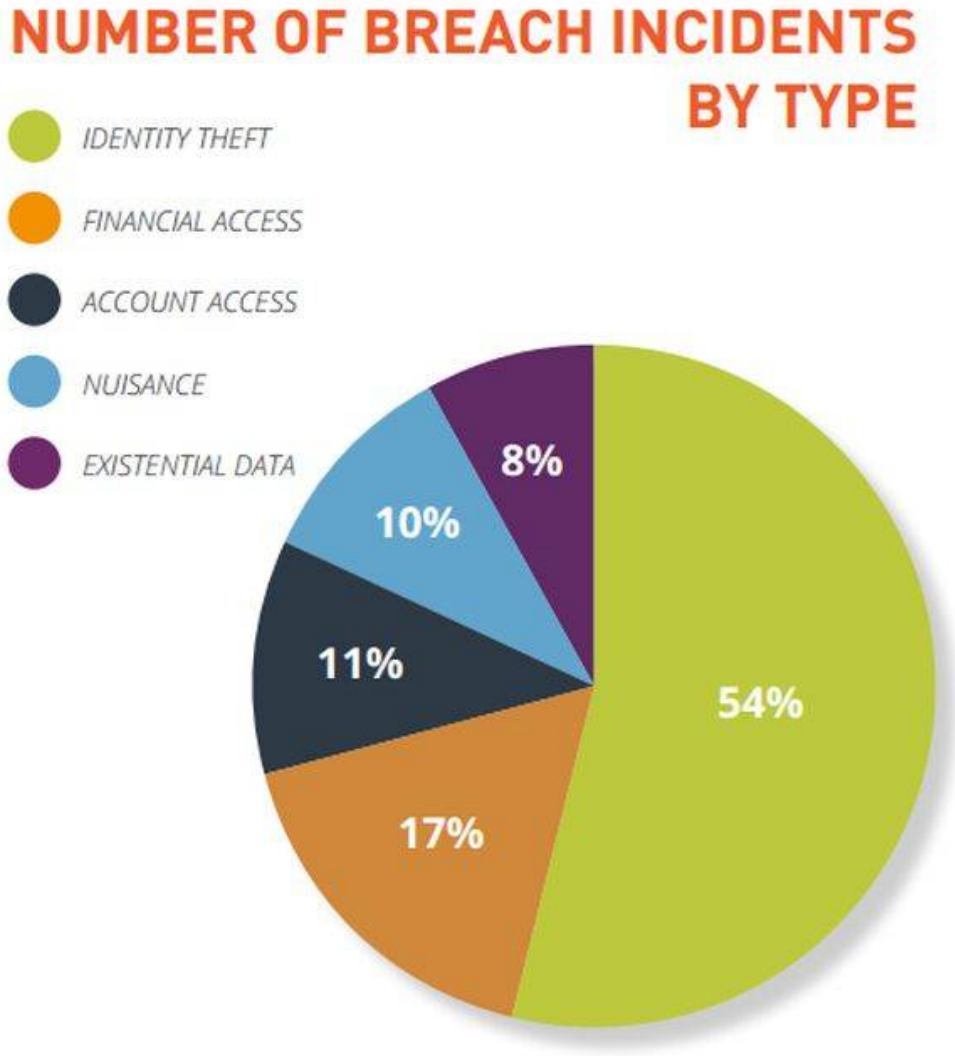
Figure 2. McAfee users have a 1 in 6 track record of downloading risky apps. Of the 8% of our users' downloaded apps that contained malware, 23% also contained suspicious URLs.

何謂手機惡意程式？

- 根據McAfee的定義，手機惡意程式指的是包含下列行為的手機程式：
  - 在未授權情況下對外傳輸資料
  - 在未授權情況下監看並記錄使用者行為
  - 傳送付費簡訊(至鈴聲下載等服務)
  - 點擊廣告(Click-fraud)
  - 濫用手機的弱點或bug去進行使用者預期之外的行為
  - 取得Root權限或安裝駭客程式，讓攻擊者得以控制手機
  - 在手機上開後門，或者讓手機成為殭屍網路的一部份
  - 從網路上下載其他的惡意程式(碼)
  - 散布垃圾簡訊
  - 毀滅手機上的資料

駭客竊取的資料種類

- 根據Gemalto調查，行動裝置遭駭客竊取的資料中，身份竊盜佔了54%，金融資料佔了17%，個人帳號資料則有11%。



法務部調查局

假關機真破壞！新Android惡意程式綁架手機關機程序

News

(iThome 2015/02/24)

AVG最近發現一款新的Android惡意程式，它能夠挾持Android裝置的關機程序，當使用者以為手機已經關機時，卻是該惡意程式運作的時候，不但能夠擅自撥打電話、拍照，還會竊取手機內的個人資料。

由於中國無法存取官方的Android程式市集Google Play，因此充斥著各種第三方的Android程式市集，也成為Android惡意程式的天堂，大多數受到PowerOffHijack感染的裝置也都出現在中國。PowerOffHijack可監聽通話內容、手機通話紀錄、手機簡訊、手機GPS位置與手機內的文件列表等。

由於PowerOffHijack必須取得最高權限才能運作，因此使用者必須刷機之後才會受到PowerOffHijack的感染，若使用Android裝置出廠時的預設韌體則能倖免於難。

想想：問題出在哪？ 如何預防？

- ✓ 不從非官方管道下載軟體
  - » 透過非官方商城(Google play, App Store)下載App（如：使用第三方商城，安裝APK檔案…等），風險較高。
  - » Google play及App Store軟體上架前必須經過審核，且有評分機制可以看見其他使用者的意見回饋，整體來說較有保障。
  - » 但不代表100%安全！
    - 根據McAfee的調查，Google Play提供的App中3%含有惡意程式

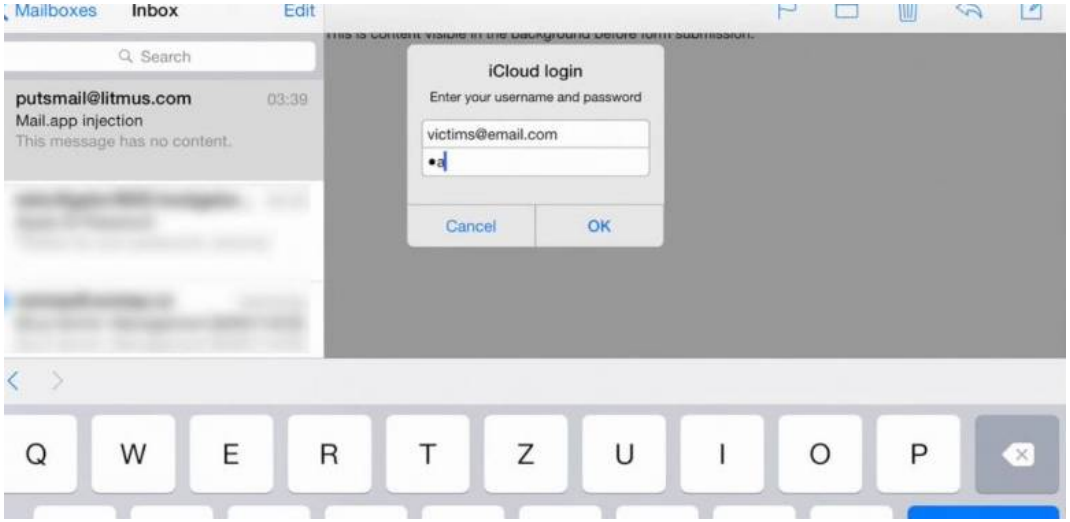
想想：問題出在哪？ 如何預防？

- ✓ 不Root/越獄(JB)裝置
  - » 不管是Android或是iOS，使用者預設都無法使用系統的最高權限
  - » 將最高權限解鎖的動作即是Root / Jailbreak (JB)
  - » Root / JB 後使用者可以使用許多預設保留未開放的功能
  - » 同樣的，也相當於將這些功能提供給惡意程式使用

News

iOS Mail漏洞
可讓駭客在郵件中遠端注入惡意程式(iThome 2015/06/12)

- 安全研究人員Jan Soucek發現，iOS版Mail應用程式有漏洞，可讓駭客藉以在郵件中載入遠端的惡意HTML內容，騙取使用者包括iCloud帳號密碼等資料。
- 蘋果官方對國外媒體表示，未接到有任何消費者受到此概念驗證攻擊程式的影響，但蘋果正在著手修補程式漏洞以便在未來更新中發佈。蘋果並表示，Apple ID的兩步驟驗證可以迫使攻擊者使用第二種無法遠端取得的驗證資料，而阻止攻擊的發生。

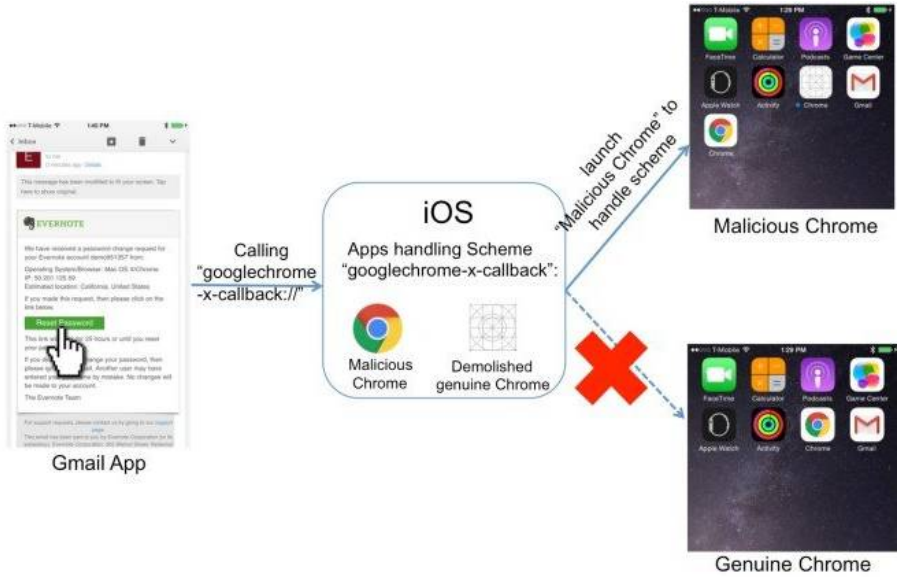


iOS出現假面攻擊漏洞：你的app就是駭客的app

News

(iThome 2015/07/12)

- 資安業者FireEye發現 iOS系統出現app的檢驗漏洞，駭客可藉以誘騙使用者下載假冒的app並偷偷取代從蘋果官方App Store安裝的合法應用程式，讓使用者的app變成駭客的惡意程式。不論是否JB都可能受到攻擊。



- 蘋果釋出的iOS 8.4解決系統上的臭蟲與安全問題，但調查顯示，迄今仍有1/3的iOS裝置並未升級到iOS 8.1.3或之後的版本而仍存在假面攻擊風險。

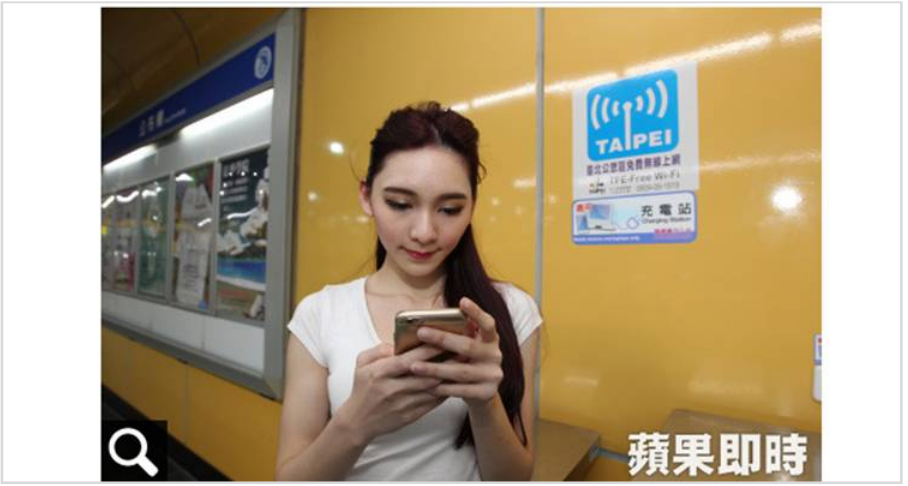
想想：問題出在哪？如何預防？

- ✓ 更新手機系統至最新版本
  - » 手機的軟體更新除了添加功能，改善效能外，更重要的是將各界回報的弱點及漏洞進行修補，未更新至最新版本的手機易受惡意程式的利用。
  - » 若是已失去支援的舊型手機，則不要在上面存取重要的資訊，並且可以考量汰換。

News

公眾WiFi防護不足　個資外洩危險大

(頻果即時 2015/05/27)



- 根據Avast Software調查顯示，台灣有 74% 的智慧型手機和平板用戶，因使用公眾Wi-Fi網路，可能導致個人的隱私外洩和身份資料遭竊的風險而不自知。
- Avast 針對台灣3700 多名消費者做調查，發現很多使用者為了避免流量超載或為求方便與快速，大多喜歡連上免費的公眾 Wi-Fi，其中有許多不需經過註冊或使用密碼；當中更有 40 % 的受訪者從不關閉 Wi-Fi 發射器或是偶爾才會關閉，而且讓行動裝置自動連上公眾 Wi-Fi 網路，如此一來等於向駭客敞開通往個人機密資訊的大門。

News

三星Galaxy手機有嚴重漏洞，超過6億手機受影響！

(iThome 2015/06/17)

- 資安業者NowSecure指出，三星手機所預載的SwiftKey鍵盤程式含有重大安全漏洞，讓駭客得以遠端執行程式碼，波及Galaxy S4/Mini、Galaxy S5與Galaxy S6等型號的三星手機，影響超過6億用戶。
- 三星於今年初釋出修補程式給合作的電信營運商，但有鑑於三星Galaxy手機經由不同的電信營運商在全球銷售，無法確定有多少營運商提供修補程式，也無法判斷還有多少三星裝置處於該風險中。
- 由於此一被預裝在三星手機上的程式無法關閉或移除，NowSecure建議尚未部署修補程式的使用者避免使用不安全的Wi-Fi網路、使用其他的行動裝置，或是向電信營運商詢問修補資訊。

想想：問題出在哪？如何預防？

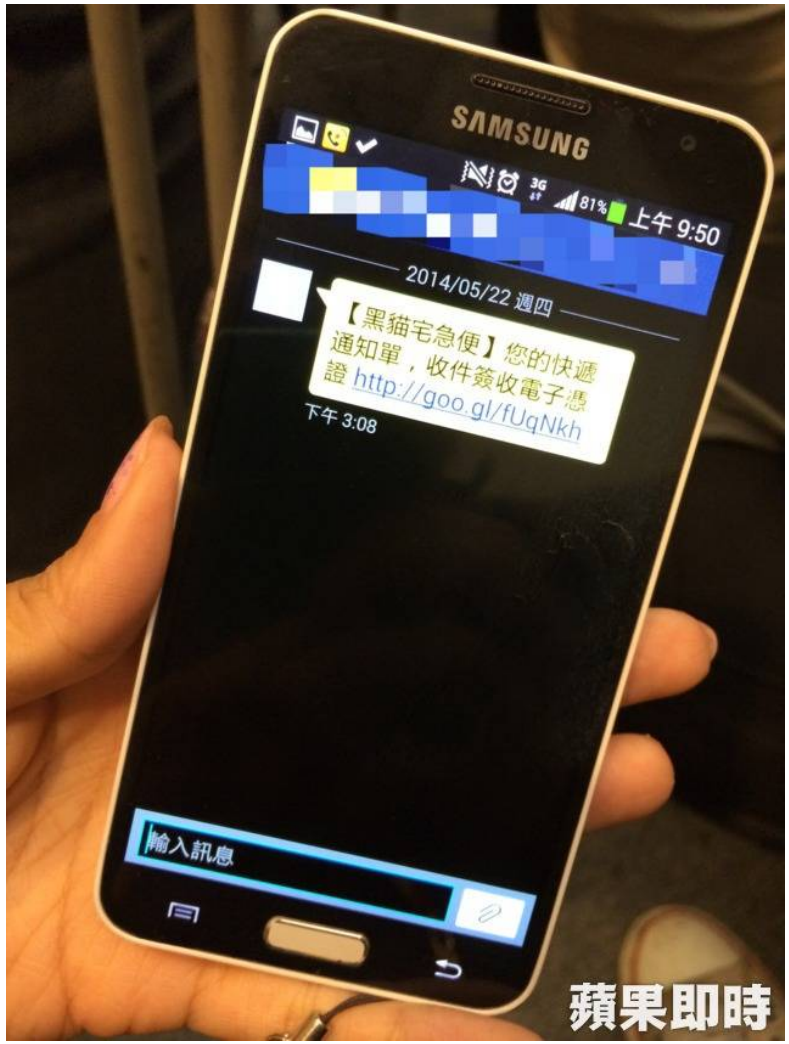
- ✓ 不使用免費公開或無安全性的Wifi
  - » 加入開放的Wifi，代表你的裝置可能跟駭客同在一個網路內，駭客可以更輕易的取得裝置的操控權，或從裡面竊取資料。
  - » 使用免費網路時，關閉自動連線的功能。
- ✓ 做好私人Wifi管理
  - » Wifi分享加上不易被猜測的密碼
  - » 無線分享器的密碼不使用預設值

News

誤按詐騙簡訊　小額付款日損5千元

(頻果日報2014/05/23)

- 許多民眾最近常會收到「【黑貓宅急便】包裹簽收電子憑證請查收」等類似簡訊，上面會附上連結，有用戶誤按後，遭到詐騙歹徒以病毒利用用戶電話號碼進行網購，民進黨立委蔡其昌今召開記者會說，目前台灣三大電信業者中華電信、遠傳電信及台灣大哥大均預先開通小額付款功能，導致用戶在中毒後，會連續收到多封小額付費認證SMS簡訊，在用戶還沒回神過來時，短時間內就遭詐騙最高一天可到5千元。



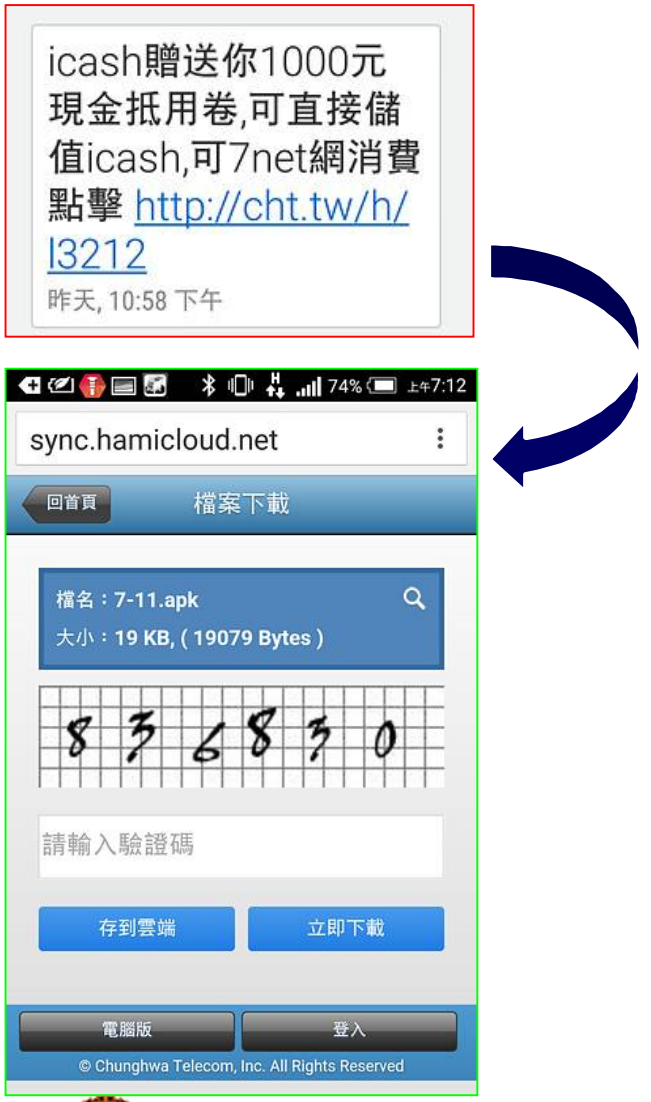
法務部調查局

News

iCash詐騙簡訊　潛藏木馬程式

(鷹眼觀察 2015/05/08)

- 民眾陳先生反應最近收到一封從0928941124 門號傳來的簡訊通知，內容寫道：「icash 贈送你 1000 元現金抵用卷, 可直接儲值icash,可7net網消費點擊 「http://cht.tw/h/l3212」。
- 然而，這其實是一個帶有惡意的詐騙簡訊。這類詐騙簡訊每一年會看到幾次，卻總是有人會直接開啟連結，甚至安裝藏在裏頭的惡意檔案，下場當然就是病毒入侵手機。而被嵌入惡意程式的手機，很可能會再傳送相同的簡訊給其他手機，達到病毒式傳播的擴散。



法務部調查局

基市副議長LINE帳號被盜 多人幫買點數被騙上萬

News

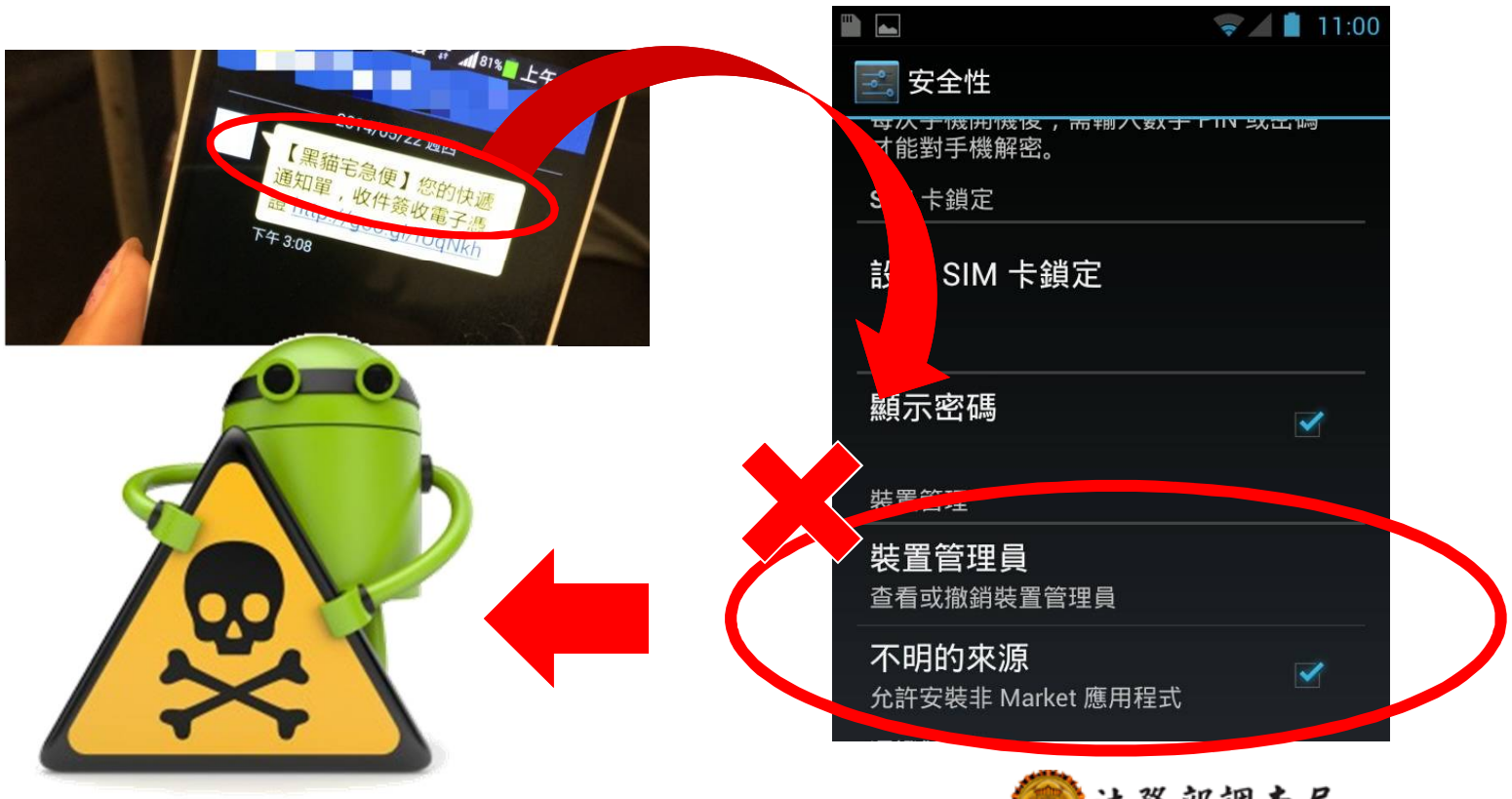
(頻果日報2014/08/23)

- 基隆市副議長宋瑋莉的LINE帳號日前遭到詐騙集團盜用，上百位親朋好友收到「到超商買幾張Gash儲值卡」的訊息，不少部屬和友人受騙上當，連遠居日本的朋友也花了5萬元日幣相挺。調查後發現，宋瑋莉可能是日前開啟不明檔案連結，手機被植入木馬病毒，導致LINE帳號密碼被盜用，目前得知已有數名幕僚、部屬和朋友受騙，損失金額從1千元到上萬元不等。

法務部調查局

想想：問題出在哪？如何預防？

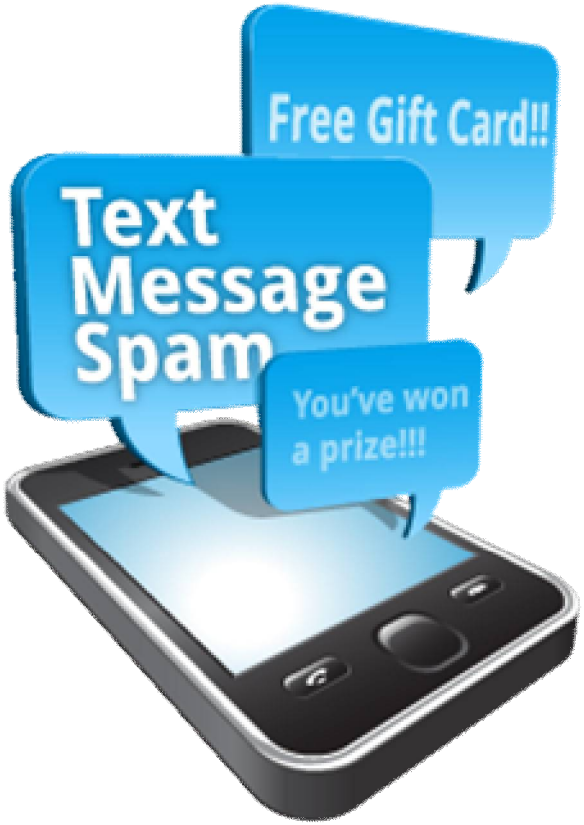
- ✓ 關閉「安裝非Market程式」功能
  - » 簡訊內的連結除了可能是小額付款的詐騙連結外，也可能連結至惡意程式的安裝檔



法務部調查局

想想：問題出在哪？如何預防？

- ✓ 再三確認訊息內容
  - » 老式的社交工程 - 詐騙簡訊手法
  - » 透過其他管道（如：電話）確認發訊息的人是誰
  - » 不點擊不明連結，尤其是經過縮網址的短連結
  - » 詐騙求證專線：165
- ✓ 不當詐騙人頭
  - » 注意手機、Line、FB帳號的安全防護，不讓有心人利用你的手機進行詐騙

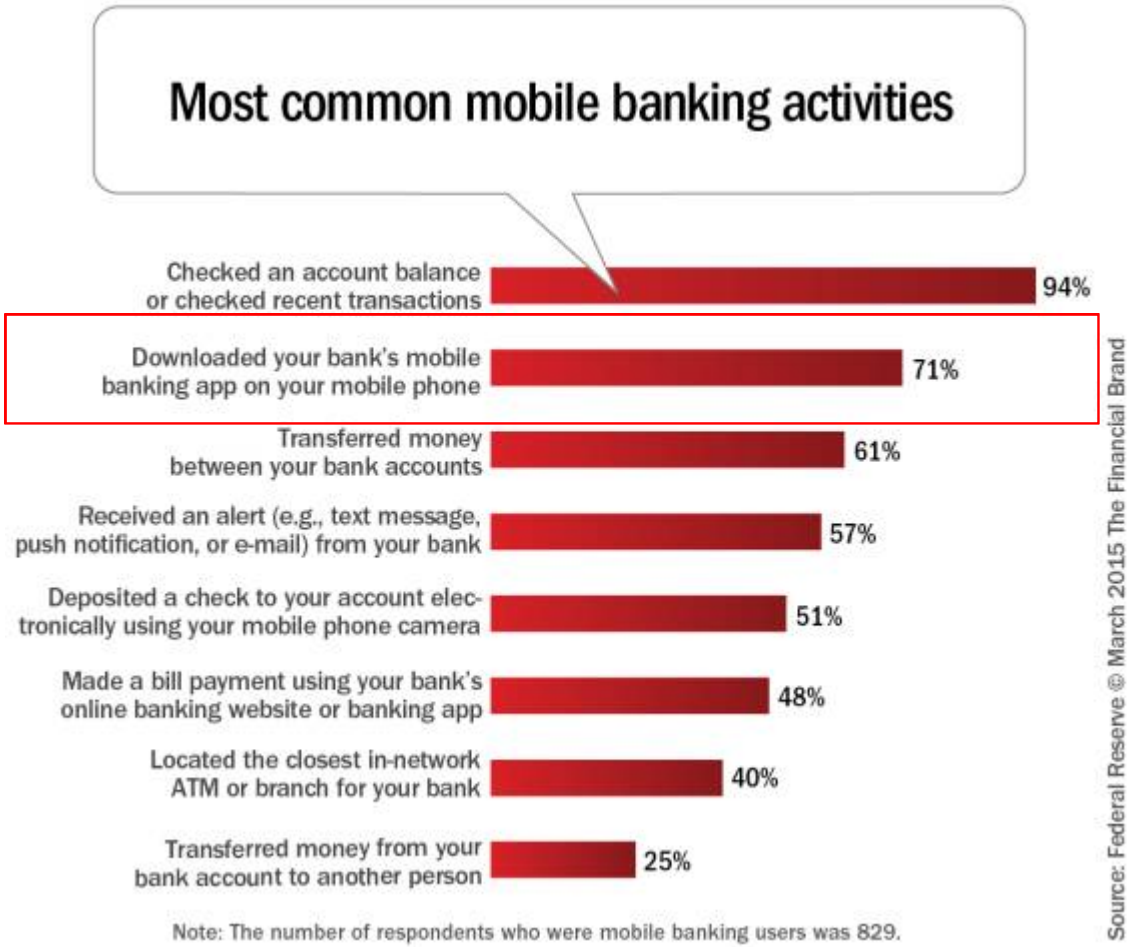


不當詐騙人頭：你是LINE帳密被盜高危險群嗎?

- **你是否有以下幾個高危險使用行為？**
  - 啟動「公開ID」功能
  - 在公用電腦登入LINE
  - 同一組帳號密碼走透透，導致Facebook等帳密遭破解，LINE也跟著被盜用
  - 沒有定期更改密碼
  - 允許手機通訊錄自動加入好友
  - 授權LINE 遊戲讀取你和好友的個人資料
  - 沒有或很少使用電腦版 LINE，卻沒關閉「允許自其他裝置登入」
- **警方提供智慧型手機自我保護方法:**
  - LINE使用者，可開啟「隱私設定」中「阻擋訊息」的功能，開啟後，不論是廣告訊息或詐騙訊息都可有效防範
  - 取消LINE「我的帳號」中「允許自其他裝置登入」，避免駭客取得帳密從電腦登入
  - 非LINE好友傳送訊息時，注意是否有不明連結，該訊息上方有「您尚未將本用戶加入好友名單內」警告，判斷是否為名單內好友
  - 打開訊息中的連結前，可先向發送訊息的朋友查證
  - 向電信公司取消小額付款功能
  - 使用Android系統的民眾，不要下載來源不明或非官方認證應用程式，應在Google Play平台下載
  - 下載應用程式時，應查看星等數、使用者評論、APP的功能及介紹、「APP存取權限」和開發者的其他APP，以免下載惡意程式
  - 如遇疑似詐騙可撥打165求證

(來源：趨勢科技)

您用過手機網銀嗎？



- 根據美國聯準會2014年12月的調查，39%的手機使用者使用手機銀行相關服務(不論從網站或是App)。
- 其中，71%的使用者下載銀行提供的行動App。

News

愛曼托行動鎖定網銀用戶，攻擊不留痕跡

(iThome 2014/07/13)

趨勢科技發現了一個名為「Operation Emmental」(愛曼托行動) 的網路犯罪行動，專門攻擊利用手機簡訊(SMS)進行雙重認證的網路銀行使用者。

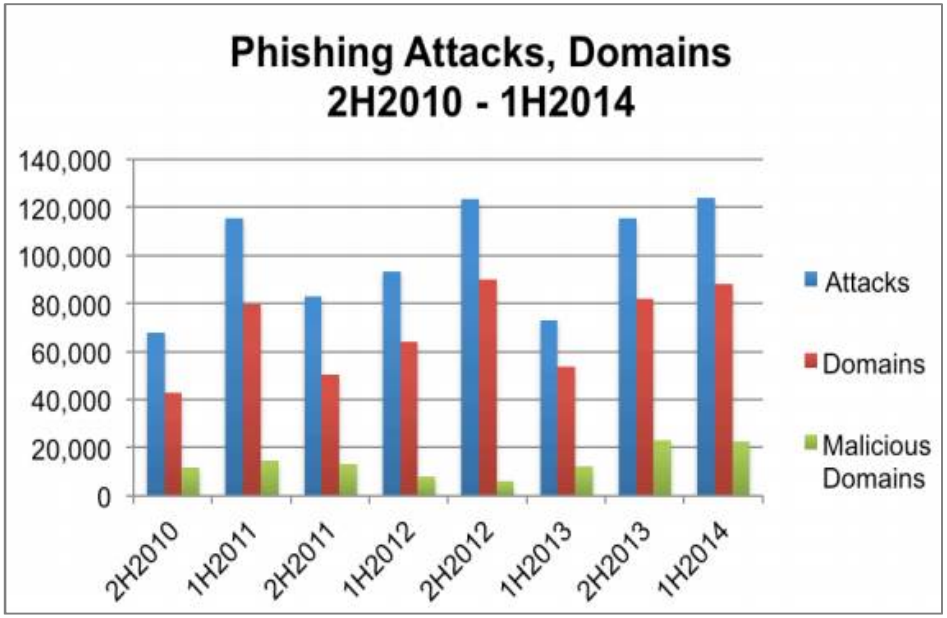
趨勢指出，該攻擊手法先以被害者所在地區的銀行或購物網站名義寄送電子郵件，誘使被害者開啟附檔後在其電腦內安裝惡意程式，使瀏覽器進入駭客的釣魚網頁時不會跳出警告訊息。

駭客再透過釣魚網頁誘騙使用者的網路銀行帳號、密碼及其他資料，要求被害者依照程序在其手機內安裝App，以App產生的**一次性密碼**輸入釣魚網頁來完成身份認證，否則便無法使用網路銀行服務。實際上該App為鎖定Android手機的惡意程式，目的是攔截真正由銀行傳送給用戶含有驗證交易密碼的簡訊，如此駭客便能盜用其身份進行網銀交易。

常見的網銀詐騙手法：釣魚(Phishing)

- 網路釣魚通常是指企圖透過電子郵件、通訊軟體來獲得你個人資訊以竊取你的身份認證。通常在訊息中會夾帶惡意連結，引導收件者至看起來與官方極為相似的山寨網站，要求提供帳號密碼等資訊。(趨勢科技)

- 2014上半年釣魚數據(APWG)
  - » 12多萬種釣魚事件
  - » 8萬7千多個網域被用來釣魚
  - » 756個企業/機構被鎖定為攻擊對象



法務部調查局

典型釣魚手法

寄件者：XX銀行【service@xxbank.com】
主旨：重要客戶通知

親愛的XX銀行客戶您好：由於我們的系統發生嚴重錯誤，導致客戶資料遺失，為避免您的網路銀行發生故障而無法使用，請填妥下列連結至的認證表格，以協助我們盡速解決此問題。我謹代表XX銀行，向您致上最高的歉意。請點選以下連結，以重新驗證您的Visa信用卡，避免您的財務損失。

http://www.xxbank.com/confirm.asp?id=123455678

XX銀行支援部 ＯＯＯ 敬啟

煞有其事的信件內容，通常是在說明事件的緊急性，要求使用者立刻輸入資料

使用縮網址或者看起來非常相似的網址

連線至網頁，或下載App要求使用者輸入帳號，密碼及其他認證資訊

News

跨平台的網銀詐騙攻擊迅速蔓延

(卡巴斯基 2014/10/17)

犯罪份子利用社交工程感染智慧型手機，即利用人性弱點，用溝通及欺騙方式，讓警覺性較低的用戶受騙上當。

在網銀通訊過程中，電腦的木馬病毒在網頁中注入惡意程式碼，並誘騙用戶下載據稱是執行安全交易必需的Android應用程式，但實際上連結會轉至惡意軟體Faketoken。一旦用戶安裝至手機，犯罪份子就能利用電腦的木馬來存取受害者的銀行帳戶，使用Faketoken攔截受害者手機簡訊的交易驗證碼，並將受害者的資金轉入自己的帳戶。

法務部調查局

想想：問題出在哪？如何預防？

» 不點擊可疑郵件中的網址

» 有疑問時，使用官方網站提供的電話進行服務

- 不要打信件中附的電話！

» 銀行不會主動要求提供登入資訊

- 永遠從官網首頁/官方手機App登入

想想：問題出在哪？如何預防？

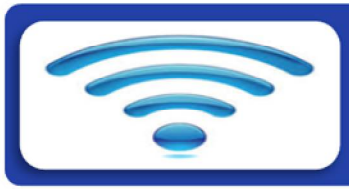
預防進階式手機網銀威脅：

- 落實電腦端的社交工程預防
  - » 留意釣魚郵件、假網址、信件附檔
- 只在官方商城內下載行動App
  - » 各大銀行的網銀App都可以在Google Play或App Store內下載到，除此之外不要安裝任何網頁要求安裝的App。
- 不在任何網銀App以外的地方輸入帳號密碼以及其他資訊
  - » 任何網頁，或是第三方的App
- 隨時將網銀App更新至最新版
- 定期更換密碼

資安意識宣導-智慧型手機安全政策

資安意識宣導—
個人使用智慧型手機安全的5不


不要自行破解手機的安全機制


不要連接不信任的無線網路基地台


不要等待，立即回報安全問題


不要跳過安全性更新


不要假設您的手機比您的電腦安全

資安意識宣導—
個人使用智慧型手機安全的5要

用Pin Code或密碼鎖定手機螢幕

安裝遠端安全服務：如遠端鎖定、清除資料或GPS定位

備份資料

儘可能加密

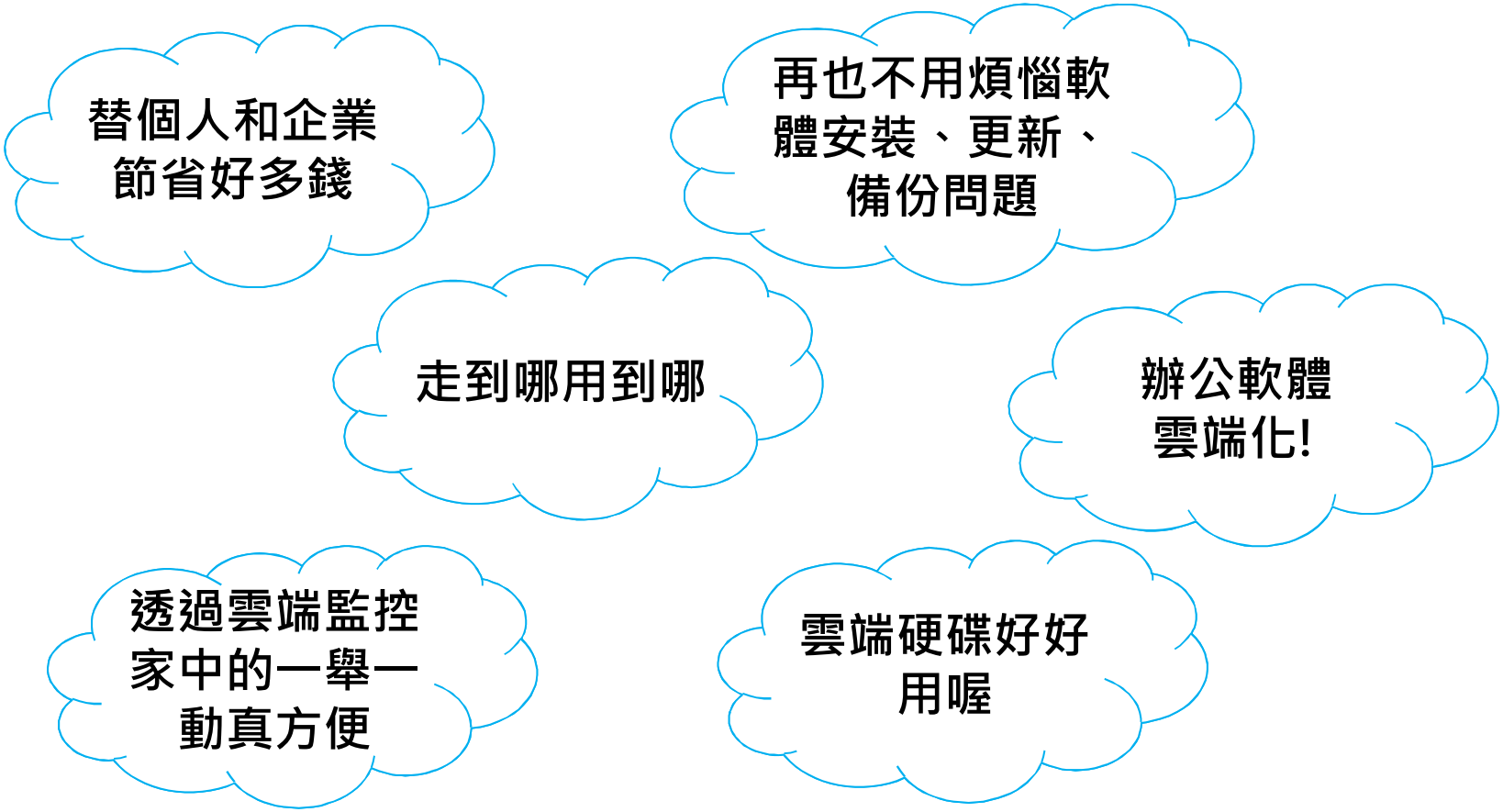
使用防毒軟體

【資安事件與案例分享】

雲端服務好方便？

雲端服務潛藏風險探討

雲端服務好方便


替個人和企業
節省好多錢
再也不用煩惱軟
體安裝、更新、
備份問題
走到哪用到哪
辦公軟體
雲端化!
透過雲端監控
家中的一舉一
動真方便
雲端硬碟好好
用喔

資安意識宣導-什麼是雲端？

NIST

雲端運算是一個模式，能便利地隨需透過網路存取設定好的共享運算資源池（如網路、伺服器、儲存裝置、應用程式與各類服務）。可以最少的管理工作或服務供應商互動，進行快速配置和發佈。

Gartner

雲端運算是一種具備大量且可擴充之IT相關能力的運算，透過網際網路技術並服務的方式(as a service)提供給外部的使用者。

Forrester

雲端運算是一種具有高度彈性、抽象的運算中心，可以提供使用者所需要的應用程式，並可依據資源使用多寡來收費。

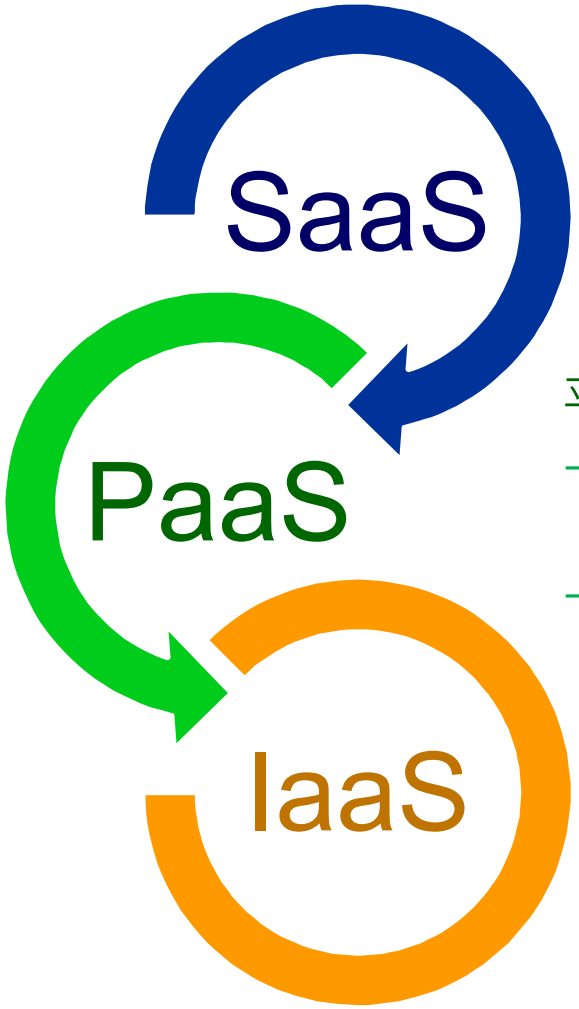
Google

應用程式和資料在雲端，可以透過任何裝置存取，使用瀏覽器在雲端間相互連通。

Wikipedia

雲端運算是種能夠將動態伸縮的虛擬化資源，透過網路以服務的方式提供給使用者的運算模式，使用者不需要知道如何管理那些支援雲端運算的基礎設施

雲端服務三大模式



軟體即服務(Software as a Service)
→ 將應用程式的功能放置在雲端上，使用者可以透過瀏覽器存取相關的服務
→ 範例：Google Docs, Gmail, Evernote

平台即服務(Platform as a Service)
→ 將環境平台放置於雲端上，使用者可以在雲端進行開發以及運行自己開發的軟體
→ 範例：Facebook App, Google App Engine

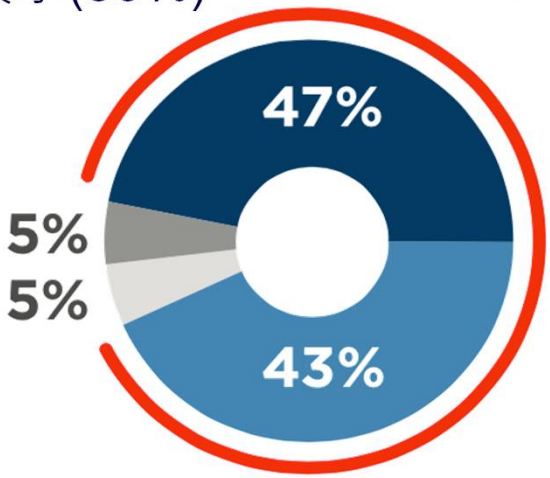
基礎設施即服務(Infrastructure as a Service)
→ 將IT基礎設施(例如: 運算效能, 儲存空間, 網路頻寬)等資源於雲端上，使用者可以在雲端執行任何電腦能做到的功能
→ 範例：Amazon EC2, HPCloud

您工作中會用到雲端服務嗎？

- 根據雲端服務廠商RightScale針對300多間企業，1000多名員工的調查...
  - » 93%的企業使用IaaS服務，或者將應用程式運行在雲端上
  - » 88%的企業使用公共雲，63%的企業使用私有雲
  - » 13%的企業有超過1000台VM在公共雲上
  - » 22%的企業有超過1000台VM在私有雲上
- 根據Nasuni於2012年底的調查，20%的員工會將公司資料存放在雲端空間(如Dropbox)上。

雲端服務真的安全嗎？

- 90%的企業對於雲端的安全性有疑慮
  - » 未授權的存取(63%)
  - » 帳號綁架(61%)
  - » 惡意員工(43%)
  - » 不安全的介面/API(41%)
  - » 服務阻斷(DoS)攻擊(39%)
- 28%的企業在雲端上碰到的安全問題比非雲端服務高
- 43%的公司允許員工在內網使用個人雲端服務(ex. Dropbox)



資料來源：Cloud_Security_Report, BitGlass, 2015

法務部調查局

News

蘋果雲端外洩裸照 101美國女星受害

(蘋果日報 2014/09/03)

- 美國好萊塢爆發女明星私密照外流風波，傳出多達101位受害人，受害女星疑似都使用蘋果iphone拍照錄影，檔案自動上傳存進iCloud，雲端資料庫icloud卻被破解入侵，才會被竊取，知名歌手蕾哈娜、加拿大小天后艾薇兒也在外洩名單中，歌壇、影壇總計上百名女星，遭到駭客荼毒。
- 這次 iCloud 漏洞導致好萊塢女星裸照大範圍爆發的主要原因是，一旦一位女星（或其身邊人）的 iCloud 帳號被攻下來之後，駭客就能夠快速恢復其帳號內的所有照片，而且還能夠通過恢復通訊錄，快速鎖定其人脈中其他有價值受害人。通過明星之間的聯繫，災難性的洩漏從此一發不可收拾。

法務部調查局

網路監視器自己說「Hello」出浴鏡頭全被駭客看光光！

News

(蘋果日報 2015/07/15)

- 今年三月台中一名輕熟女在套房裝網路監視器，以便外出時透過手機觀看愛貓動態。日前卻發現有不明人士駭進系統，她拿手機邊走邊登入，竟發現登入人數是二人，且手機監看畫面停留在她的身上，「我想閃躲鏡頭，機器卻跟著轉，嚇得我用手按壓它並蹲下將電源拔掉」她事後退貨並報警，同時趕緊和一起團購的朋友聯絡，結果十四個買家中竟有三人出現類似情形，有一名朋友甚至聽見監視器說：「hello!」。

- Webcam（網路監視器）是一種可透過有線或無線網路傳輸影像的攝影機，使用者可透過電腦軟體或手機App，輸入帳號、密碼，經伺服器認證即可連上Webcam，將即時畫面傳回電腦或手機。無論人在何處都可遠端監控錄影。

法務部調查局

News

資安專家警告政府內網防護有盲點，Dropbox成遙控潛伏傀儡電腦新跳板(HITCON 2015/07/07)

隨著雲端儲存的普及，有許多政府機關也善用這類雲端服務，增進資料交換的效能。不過，叢培侃表示，今年上半年在臺灣政府機關發現，駭客利用修改自開放原始碼DropNet的惡意程式，連線Dropbox、Google硬碟等雲端儲存服務儲存駭客的控制指令，藉此遙控政府內部的傀儡電腦。

這個DropNet惡意程式本身沒有設定其他的C&C等中繼站資訊，透過連到Dropbox、Google硬碟等各種雲端儲存空間，接受駭客的指定訊息。因為所有的通訊都是採用HTTPS加密連線，包括各種網路閘道端的檢測設備，都無法解析加密連線的內容，加上，這個惡意程式是用開放原始碼的DropNet修改，一般的防毒軟體也都不會預警。目前常見植入受駭電腦檔案包括：igfxpres.exe、DropNet.dll和dropbox.exe。

在分析這個修改自DropNet的惡意程式時，叢培侃表示，該惡意程式最大的缺點在於，駭客解碼的令牌（Token）必須寫死在程式碼中，所以，資安鑑識人員只要可以找到感染到該惡意程式的電腦做鑑識分析，就可以看到有哪些受駭電腦。目前許多重要機關電腦都有被植入這個惡意程式，也可以遠端遙控傀儡電腦，他說：「除非機關單位中斷所有雲端儲存服務的連線，否則，目前很難有好的防護方式。」

News

OO黨遭駭雲端硬碟 選舉機密全外流

(中國時報 2015/06/20)

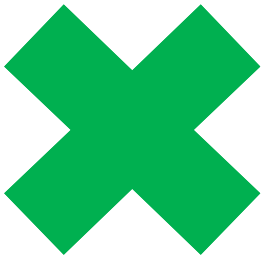
- 不管按幾次重新整理，網路頁面始終停留出現錯誤訊息，OO黨新聞部主任黃OO，拿出筆記型電腦加上WIFI才能開始處理公事，沒想到連信箱，都是駭客攻擊目標。
- OO黨新聞部主任黃OO表示：「我剛改完(密碼)的時候，準備使用十分鐘之後，我的帳號密碼又被改了！所以你可以知道說，地球上某個角落，有個人同時在跟著你，在做同步作業，其實還蠻害怕！訪美前包括我們的秘書長，其實所有主管通訊軟體用LINE，寄了一封信跟我講說，我的帳號已經在另外一個人，手機上被登入。」

雲端運算的七大安全威脅

- CSA (Cloud Security Alliance) 在 (2010 年 3 月) 初發布了一份研究報告，提出目前雲端運算的七大安全威脅：

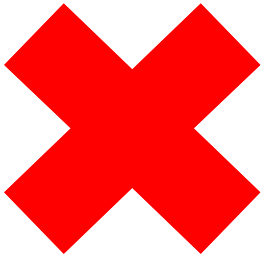
1. 濫用或利用雲端運算進行非法的行為
2. 不安全的介面與 APIs
3. 惡意的內部人員
4. 共享環境所造成的議題
5. 資料遺失或外洩
6. 帳號或服務被竊取
7. 未知的風險模型

資安意識宣導-
培養使用雲端服務的好習慣



- 不用
  - » 不在辦公環境內使用私人雲端服務

- 不存
  - » 不將公務資料存放於私人雲端服務之上



- 不分享
  - » 設定好共用權限，不將具有機密性的資料分享

資安意識宣導-
常見雲端服務企業風險管理議題

- 雲端管理議題

法律遵循

- 服務服務商所提供之服務是否符合法規要求
- 資料保存與銷毀是否是否能符合資料所在位置的隱私保護政策
- 發生法律訴訟時如何提出證據

資訊安全

- 資料是否在不知情的情況下被察看或存取
- 是否能確保資料在災難中不受損害
- 資料存放地點與設備的實體安全是否受到適當保護

服務可用性與穩定性

- 服務服務商是否能提供提供長時間不中斷的服務與永續之經營
- 服務服務商是否能夠支持日益增長的需求，提供之可靠服務
- 業界缺乏共通標準，系統之移轉將受到限制

Deloitte.
勤業眾信

資訊安全宣導

- 進行宣導前，請您先想想看～
  - 日常作業中如何做好資訊安全？
  - 遵循資訊安全你我皆有責任？

沒有百分之百的資訊**安全**，

得靠**每個人**從**小地方**一起努力！

1.不明人士要盤查

- 不明人士，在辦公區域內走動，應該主動詢問其來意。
- 發現可疑狀況應加以制止或通知相關人員處理。
- 即使是認識之同仁，進出其沒有權限出入之區域，也要加以勸阻或通知相關人員處理。
- 委外服務人員出入本局，應一律配掛臨時工作證並遵守門禁之規定。
- 委外服務人員進入本局時，應直接到指定之工作區域，禁止到非工作區域；離開時，應直接出大門，禁止在本局內逗留。

2.電腦不用要登出(1)

- 離開座位，電腦應該設定螢幕保護程式（須設定開機密碼，時間最長不得超過20分鐘）或是其他控制措施保護
- 離開座位致所使用資訊設備有遭入侵之虞者，應於離開前將螢幕鎖定
- 長時間離開辦公室，建議將電腦關機
  - » 杜絕來自網路破壞
  - » 防止帳號或密碼被盜用
  - » 防止重要資料遭竊

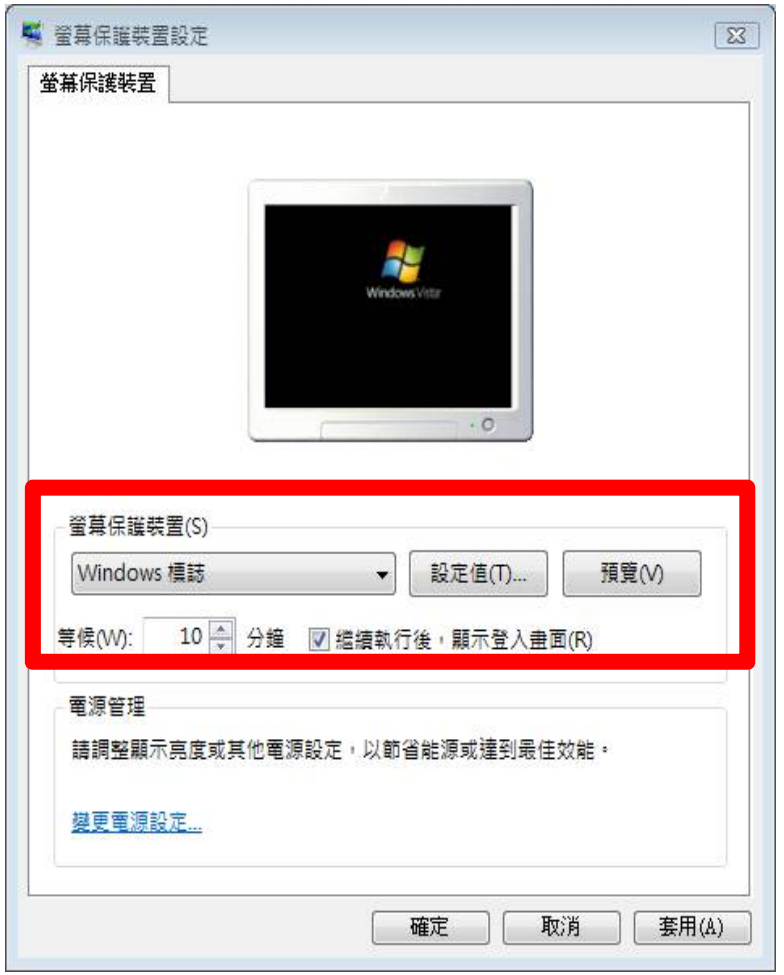
2.電腦不用要登出(2)

自我檢查

- 檢查作業系統之「螢幕保護程式」設定，確定一段時間未動作後會進行鎖定，避免他人誤用。

執行重點

1. 檢視是否依單位規定時間已設定「等候時間」。
2. 檢視已勾選「繼續執行後，顯示登入畫面」項目。
3. 若單位內以AD目錄服務進行控管，檢視GPO之設定是否包含「螢幕保護程式」設定。



3.機密資料要保護(1/2)

- 員工可能會把機密性資料文件、備忘紙、以及記載個人相關資訊等文件，隨意放置於桌上。
- 或者將資料進行完善的分類，並且儲存在電腦桌面上，這些動作都很容易導致資料的外洩。
- 因處理業務保有敏感性、機密性電腦資料或檔案者，應加強安全保護措施，如下班時應該上鎖或以其他方法妥為收存。

3.機密資料要保護(2/2)

- 連接網際網路的個人電腦、筆記型電腦
  - » 不得處理機敏公務
  - » 不得放置機敏公務資料
  - » 禁止連接儲存機敏公務資料之可攜式儲存媒體（磁片、光碟片、隨身碟、外接式硬碟等），以防止後門（木馬）程式竊取資料
- 避免**USB儲存裝置**讓電腦系統感染病
  - » 預防電腦病毒傳給USB儲存裝置
    - 建議：在USB行動碟內建立 autorun.inf (ini) 資料夾
  - » 避免USB儲存裝置傳病毒給電腦
    - 關閉USB儲存裝置自動執行設定（Auto Run）
  - » 常見USB儲存裝置病毒
    - kavo.exe, taso.exe, mpsvbtk.exe, wjftxbl.exe, meex.exe, hfhludy.exe

4.重要資料要備份

- 不論是紙本或電子檔的重要資料，皆應：
  - » 定期備份
  - » 存放在不同地方(異地備份)。
- 資料備份原則
  - » 資料價值較高時應優先備份。
  - » 選擇適合之儲存媒介進行資料備份工作。
  - » 按所欲備份的資料型態，選擇方法進行備份(如：完份、漸進式(增量)備份)。
  - » 備份的資料需定期做資料回復測試，以確認備份資料的可用性。

5.電腦防毒要更新(1/2)

- 電腦中毒徵兆：
  - » 電腦系統運行速度異常緩慢。
  - » 上網速度越來越遲緩。
  - » 異常的系統訊息通知。
  - » 螢幕顯示異常，例如畫面突然一片空白。
  - » 來自防毒軟體的警告訊息。
  - » 電腦無故自動關機或不斷重新開機。
  - » 瀏覽器自動出現產品廣告或色情網頁。
  - » 網路流量異常，例如沒有使用網路服務或收發電子郵件，但網路的連線燈號卻一直閃爍。

5.電腦防毒要更新(2/2)

- 防毒軟體的偵測與防範功能只有在該軟體有在運作、且有時常更新病毒碼情形下，才會產生效用。
- 防範訣竅：
  - » 隨時注意防毒軟體的病毒碼是在最新的狀態（四個病毒碼版本之內，如有問題立即連絡單位資通安全業務承辦人員）。
  - » 安裝防毒軟體或反間諜軟體。
  - » 不關閉、不刪除防毒軟體。
  - » 定期執行掃毒。
  - » 不要隨意複製或下載不明檔案。
  - » 不要隨意開啟檔案。

6.應用系統要更新(1/2)

- 當軟體被使用一段時間後，通常會出現一些小問題或安全漏洞，這些漏洞也是駭客容易利用的弱點，零時差攻擊即目前駭客最喜歡利用的手法。
- 防範訣竅：
  - 檢查以下重要應用程式或軟體是否為最新版本：
    - 作業系統(Windows 7 或2000、Mac、Linux...等)
    - 網頁瀏覽程式(IE、FireFox...等)
    - 辦公室應用軟體(Office、Adobe PDF...等)
    - 電子郵件收發軟體(如outlook、outlook express...等)
- 大部分的軟體都會提供一項「自動更新」功能，啟動自動更新功能為最方便也最迅速的一種定時更新方法。

6.應用系統要更新(2/2)

自我檢查

- 檢查作業系統之「Windows Update」是否已更新至最適狀態。

新增或移除程式

執行重點

1. 作業系統進行Windows Update前，是否先進行測試，確認新版修補程式(Path)不會影響系統服務提供，才佈署至正式環境。

2. 是否定期檢查電腦之更新狀態，確保無系統長期未安裝修補程式之情事發生。(尤其新進同仁所配發之個人電腦)。

3. 檢視作業系統變更程序文件
   - 使用者帳號異動控管。
   - 作業系統物件與存取權限異動控。
   - 作業系統檔案內容存取控管。

7.使用網路要注意

- 公務電腦原則上限公務使用，且必須加入網域。
- 不得任意更改個人電腦IP 位址與網路卡。
- 個人電腦不得安裝數據機或架設無線網路等相關對外連線設備。
- 非經本局同意不得自行與外界網路相連結；未經核准不得於本局網路私自架設網站。
- 不得將私人個人電腦、筆記型電腦連接公務網路(內外網)。
- 除因公務需要且經本局核可外，不得使用點對點（Peer-to-Peer, P2P）分享軟體。

8.電腦軟體要授權

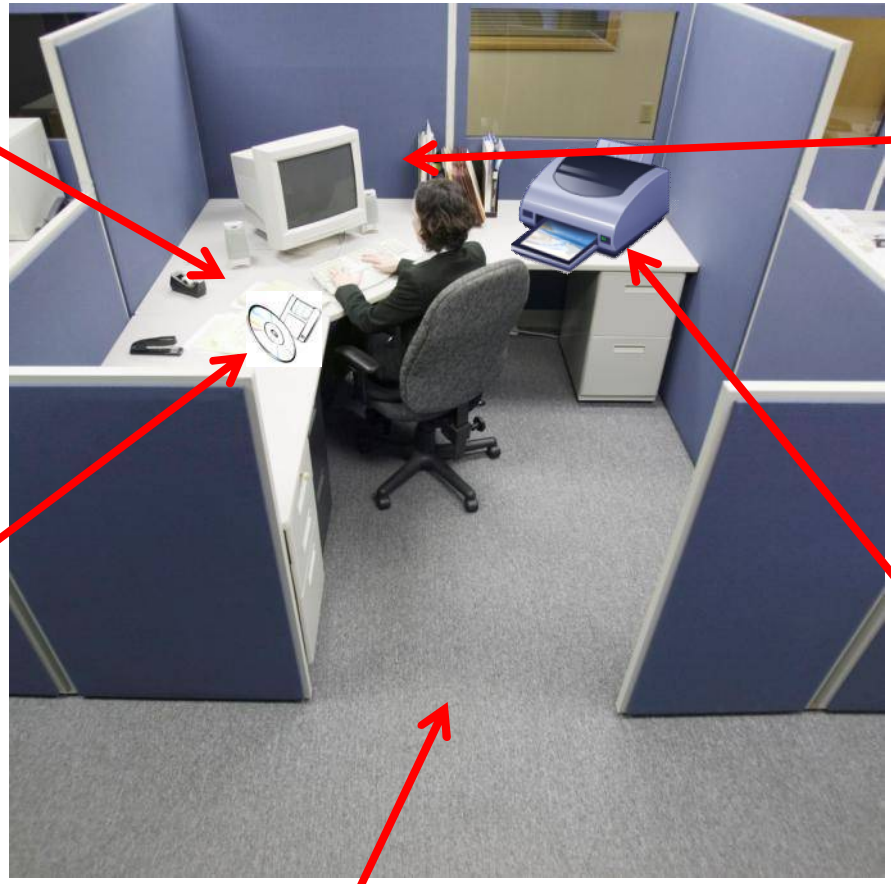
- 個人電腦原則僅安裝業務所需軟體，安裝前應確認取得合法授權。
- 連接網際網路之電腦，不得安裝本局公務使用之軟體，亦不得有本局標識之圖示或機關銜稱。
- 不得將授權軟體轉借或給予未經授權人員使用。
- 不得任意移除或卸載本局所安裝之資安防護軟體。
- 使用私有、試用、免費或共享軟體時應考量系統安全性，避免危及本局電腦或網路的安全。
- 如發現使用非授權的軟體，由使用者自行負相關法律責任。

9.資訊傳輸要注意

- 機密性資料及文件，不得以電子郵件或其他電子方式傳送
- 機密性資料以外之機敏性資料及文件需以適當的加密或電子簽章等安全技術處理
- 應確認對方的郵件地址，不要隨意轉寄未確認來源之信件
- 機密文件以人工傳遞需妥善保護（如：專人親送、密封）
- 機敏性資料及文件以書面方式傳遞時，須密封交專人傳遞，封套應註明收件人，並由其當面簽收，嚴禁他人拆封。

資訊安全宣導 - 辦公室設備使用注意事項

- 離開座位時，機密文件不應置於辦公桌
- 下班前需清理工作場所



- 電腦閒置時，應設定螢幕保護程式或鎖定螢幕
- 不應將使用者之帳號密碼紀錄於紙本
- 定期檢視防毒軟體及Windows Update是否確實更新

- 儲存媒體(如USB隨身碟)應妥善保管
- 使用、移動及存取多媒體應遵循管制程序
- 報廢的儲存媒體需確實銷毀

- 印表機、影印機應有專人負責
- 紙本文件回收前應確認是否含有機密資訊
- 文件銷毀需確實
- 會議後須將會議室桌面及白板淨空

- 限制區域應有門禁管制非經允許與陪同，外部人員不得進入
- 辦公區域檔案櫃、抽屜、辦公室應上鎖

動動腦時間

- 前面的資訊安全觀念還記得嗎～
  - 接下來10分鐘，將進行10題練習，以檢視各位學習的成果~

一般人員資安宣傳教育訓練測驗

- _____1. 防毒軟體將拖累系統效能，平日可先關閉常駐防毒軟體，當要掃毒時再開啟即可。
  - X (正解：防毒軟體應保持啟動運作狀態，以確保防毒功能之有效性)
- _____2. 軟體即服務(Software as a Service)係指將應用程式的功能放置在雲端上，讓使用者可透過瀏覽器進行存取之服務，如：Google Docs, Gmail, Dropbox, Evernote。
  - O(正解：軟體即服務(Software as a Service)是雲端服務三大模式之一，是指將應用程式的功能放置在雲端上，使用者可以透過瀏覽器存取相關的服務。)
- _____3. 濫用手機的弱點或bug去進行使用者預期之外的行為屬於手機惡意程式的一種。
  - O (正解：根據McAfee的定義，手機惡意程式包含濫用手機的弱點或bug去進行使用者預期之外的行為。)

一般人員資安宣傳教育訓練測驗

- _____4. 為避免網站帳號密碼使用太多組而忘記，各網站皆可使用同一組帳號密碼。
  - X(正解：各網站應使用不同帳號密碼，避免一組網站帳號密碼被竊因而波及所有的網站)

- _____5. 如撿拾不明隨身碟，最好是放入電腦中讀取，看是否有失主的聯絡方式。
  - X (正解：不明隨身碟恐含有惡意程式碼，直接在電腦上使用，可能造成病毒感染)

- _____6. 電腦系統運行速度異常緩慢是電腦可能中毒的徵兆之一。
  - O (正解：電腦可能中毒的徵兆包含電腦系統運行速度異常緩慢)

一般人員資安宣傳教育訓練測驗

- _____7. 透過官方商城(Google play, App Store)下載App（如：使用第三方商城，安裝APK檔案...等）風險較低，但不代表100%安全。
  - O(正解：Google play及App Store軟體上架前必須經過審核，且有評分機制可以看見其他使用者的意見回饋，整體來說較有保障。但根據McAfee的調查，Google Play提供的App中3%含有惡意程式)

- _____8. 使用電子郵件時須檢查寄件者的真偽，只須確認寄件者名稱即可，無須檢查寄件來源地址。
  - X (正解：檢查寄件者的真偽，不但須確認寄件者名稱，亦須檢查寄件來源地址是否經過偽造)

一般人員資安宣傳教育訓練測驗

- _____9. 為避免忘記密碼，而帳號慘遭系統鎖死，可在桌面及電腦螢幕張貼電腦帳號及密碼紙張。
  - X (正解：為避免帳號遭有心人士竊取，切勿在桌面及電腦螢幕張貼電腦帳號及密碼紙張。)

- _____10. 通訊軟體用來討論工作及傳輸檔案可增進辦公效率且安全。
  - X(正解：使用即時通訊談論公事及傳輸檔案，有潛在資安危害，應避免於辦公環境使用即時通訊，可降低資訊外洩風險。)