永遠走在最前面
Always Ahead

基隆市政府暨所屬機關
108年度資通安全基礎教育訓練

資安顧問
唐世智/黃金榜/林宗鈞/方依欣

中華電信
Chunghwa Telecom

大　綱

壹 資通安全法概論

貳 資安與個資事件分享

參 社交工程與行動裝置安全管理

肆 資安事件通報規定及宣導

伍 資安政策宣導

NCCSC揭牌
總統：資安即國安的具體實現

資料來源：央廣新聞 107.11.15 https://www.youtube.com/watch?v=TX4HH9paMy4

國家資通安全發展方案(106-109年)

願景	打造安全可信賴的數位國家			
目標	建構國家資安聯防體系 提升整體資安防護機制 強化資安自主產業發展			
推動策略	完備資安基礎環境	建構國家資安聯防體系	推升資安產業自主能量	孕育優質資安人才
具體實施	1. 完備我國資安相關法規及標準 2. 強化基礎通訊網路韌性及安全 3. 建立政府資安治理模 式	4. 強化關鍵資訊基礎設施資安防護 5. 建立跨域資安聯防機制 6. 精進網路犯罪防制能量	7. 發展新興資安產業 8. 輔導資安產業升級 9. 鏈結產學研能量發展新興資安技術	10. 增加市場資安人才供給 11. 提升政府資安人力專業職能

資料來源：行政院國家資通安全會報 106.11

立法目的及規範對象

➢立法目的

- 由於公務機關所承擔之公共服務，及關鍵基礎設施提供者所提供之服務，均對國家安全、民眾生活、經濟活動等有重大影響•
- 藉由立法課予前述該等機關之資通安全維護責任，以保障國家安全，維護社會公共利益

➢規範對象

公務機關

•中央與地方機關(構)
•公法人

特定非公務機關

•關鍵基礎設施提供者
•公營事業
•政府捐助之財團法人

立法目的及規範對象

➢排除對象

- 資安管理法第3條第5款 公務機關：指依法行使公權力之中央、地方機關(構) 或公法人。但不包括軍事機關及情報機關。
- 資安管理法施行細則第2條 所稱軍事機關，指國防部及其所屬機關(構)、部隊、學校；所稱情報機關，指國家情報工作法第三條第一項第一款規定之機關。

資通安全管理法推動歷程

106/4 行政院完成審查並將法案函送立法院審查

5 於立法院第九屆第三會期完成一讀程序並交付司法及法治委員會審查

107/3-5 研擬子法草案並召開分區座談會

5/11 立法院第九屆第五會期二、三讀通過立法

6/6 總統令公布

7/9 子法預告

11/21 子法發布

108/1/1 正式施行

108下半年 關鍵基礎設施提供者納管施行

01 廣納政府機關意見

02 與專家學者交換意見

03 與業者溝通

04 向大眾說明

05 與國會溝通

資料來源：行政院資通安全處

資安法法案結構

主管機關(行政院)應辦事項

立法目的與名詞定義

公務機關資通安全管理

國家安全
社會公共利益

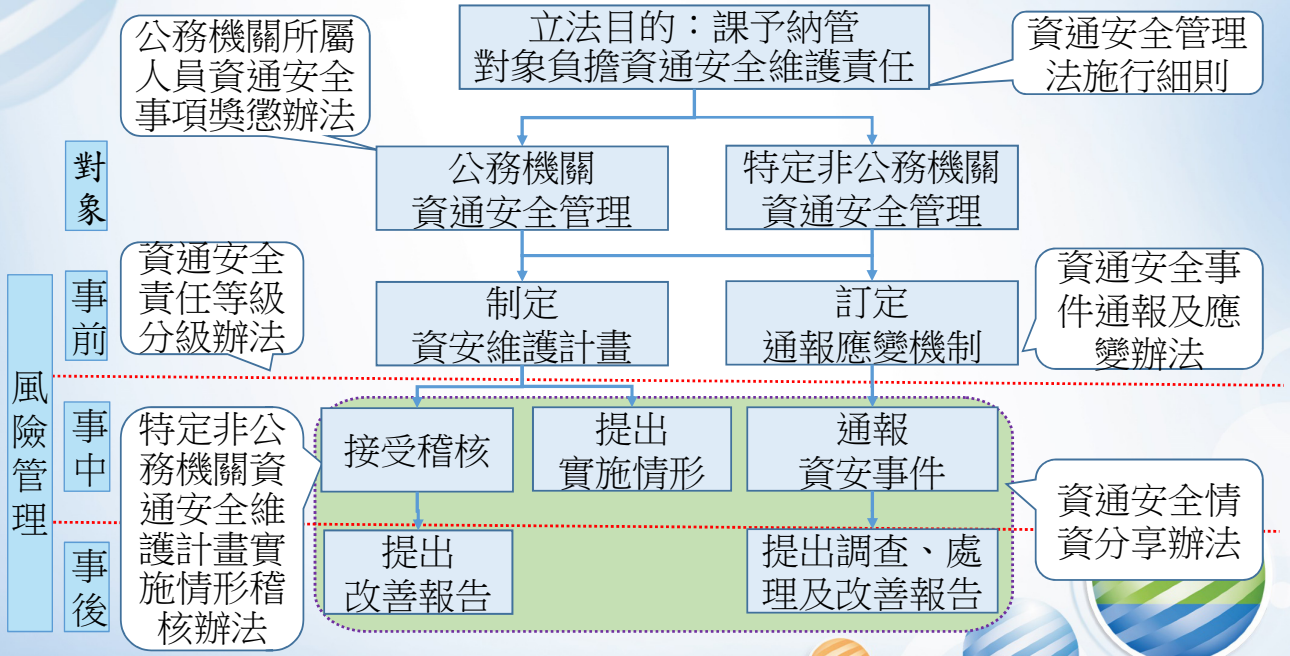
罰則

特定非公務機關資通安全管理

資料來源：行政院資通安全處

關鍵基礎設施(CI)

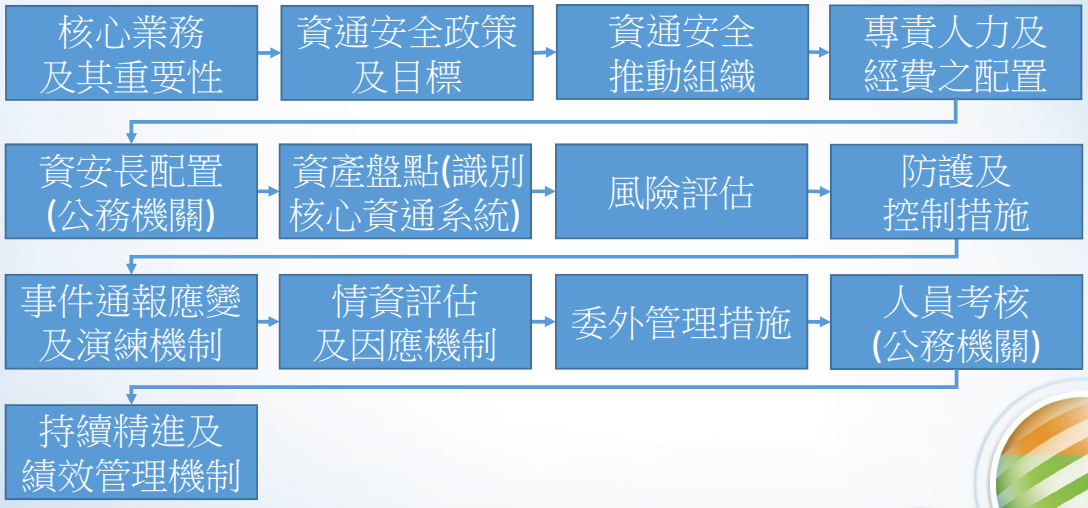
資安管理法及六項子法架構



資料來源：行政院資通安全處

資通安全維護計畫內容

• 基於風險管理之基礎，包含下列內容(13款)



大　綱

壹 資通安全法概論

貳 資安與個資事件分享

參 社交工程與行動裝置安全管理

肆 資安事件通報規定及宣導

伍 資安政策宣導

資安重要性及資安威脅影響面

- 網路帶給人們便利的生活，可以透過網路訂餐、買衣服、買賣(租)房子、訂車票、線上課程、線上遊戲、監視器、無紙化辦公……
- 現今的時代，食衣住行育樂可以說是與網路密不可分。
- 網路讓生活更便利、更豐富，但也帶來了相對應的危機，資訊安全人人有責，想要避免發生資安事件(事故)，就須從日常中做起。

快改 IG、FB 密碼！臉書坦言上億用戶密碼員工看得見

- Facebook 稍早發出新聞稿提及自家的資安新政策，同時承認在今年 1 月，臉書發現部份用戶的密碼，被以可以完全看見的形式儲存在內部系統，導致臉書員工可以隨意瀏覽用戶的密碼，進而產生資安風險。
- 受到影響的用戶數量，包括數億個 FaceBook Lite 帳戶、其他數千萬個的 Facebook 帳戶，以及數萬名 Instagram 用戶。

資料來源：https://today.line.me/tw/pc/article/快改IG、FB密碼+上億用戶密碼曝光-2rqQ06

2019/03/22

快改 IG、FB 密碼!
臉書坦言上億用戶密碼員工看得見

- 網路安全解決方案廠商Check Point的研究人員近日在Google Play商店中出現了新型態的惡意廣告軟體「SimBad」，目前已知有高達210款應用程式受害，其中模擬類手遊占最大宗，這些應用程式的總下載次數高達1.5億次，Google指出，目前這些受害的應用程式皆已遭下架。
- Google方面表示，目前已經掌握相關狀況，且已經移除所有在Google Play商店中被感染的應用程式，Check Point指出，大部分被感染的應用程式都是模擬類手遊，大他們推測，大部分開發者們應不知道SimBad背後的相關惡意機制。
  SimBad還有釣魚連結、打開特定App進行攻擊等風險。

資料來源：https://today.line.me/tw/pc/article/Google+Play+210款應用程式有病毒+第三方能入侵Android手機-M27xYM 2019/03/22

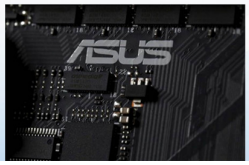
NASA伺服器遭駭客入侵

- 美國太空總署(National Aeronautics and Space Administration, NASA)在2018/12/18發布了內部通知，指出他們在2018/10/23發現有駭客入侵了NASA用來存放員工資訊的伺服器，在2006年至2018年間任職NASA的員工資料恐已外洩。這封內部通知信還被公開到媒體上，才讓這起事件曝光。根據NASA的初步調查，駭客存取的其中一台伺服器存放了員工的社會安全碼與其它的個人身分資訊，受到影響的是NASA內身分為公務員(NASA Civil Service)的員工，只要是在2006/7至2018/10上任、在職或轉換單位的員工都受到波及。在發現這起意外之後，NASA立即採取措施來保護伺服器與資料，並與聯邦網路安全專家聯手展開調查，目前仍在評估資料外洩規模，尚未有確切的數據，僅強調NASA的任務並未受此一入侵行為的影響。

資料來源：https://www.zdnet.com/article/nasa-discloses-data-breach/

遭爆百萬台電腦遭駭？華碩：僅數百台受影響

- 外媒披露，華碩去年在更新伺服器時遭駭客植入惡意後門病毒，估計受影響的電腦達上百萬台。華碩則表示，經調查目前只有數百台受影響，且已主動聯繫此部份用戶。
- 卡巴斯基是在今年1月，使用了新的供應鏈檢測技術後，進而發現這起安裝後門病毒事件，駭客攻擊的時間應是發生在2018年6月到11月間。
- 華碩指出，Asus Live Update工具程式可能遭受特定APT集團攻擊，並指出這類攻擊手法，主要針對特定機構用戶進行攻擊，較少是針對一般消費用戶。
- 針對此次攻擊，華碩進一步說明，已對Live Update軟體升級全新的多重驗證機制，以確保這樣的入侵事件不會再發生。



資料來源：中時電子報 2019/03/26

Android防毒軟體只有3成有效，更有2成5反而不安全

- 行動上網病毒防不勝防，Android手機用戶可能想到下載防毒強化手機安全。不過一項研究顯示，連Google官方的Play Store上的防毒軟體或反惡意程式軟體，僅三分之一具備一定水準的防護能力，其他的不是偽造程式，就是沒什麼效果，更有24%屬於不安全的程式。
- 國際獨立測試機構AV-Comparatives今年一月針對Google Play Store上250款反惡意程式app做了測試。研究團體讓所有app在同樣條件下偵測新近2000隻惡意程式樣本。
- 測試結果中，有80款app對惡意app偵測率超過30%，列入前段班。包括MalwareBytes、AVG、Avast、Avira、Bitdefender、Qihoo、ESET、F-Secure、Sophos、TrendMicro、卡巴斯基、McAfee以及Google Play Protect等都上榜了。

資料來源：https://www.ithome.com.tw/news/129367 2019/03/15

大　綱

壹 資通安全法概論

貳 資安與個資事件分享

參 社交工程與行動裝置安全管理

肆 資安事件通報規定及宣導

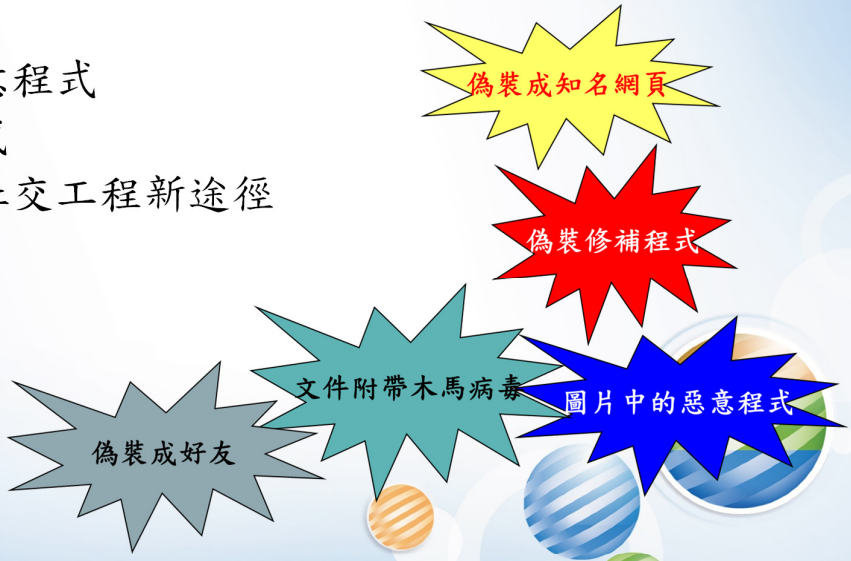
伍 資安政策宣導

社交工程

- 何謂社交工程 (Social Engineering)
  - 利用影響或說服力，以欺騙他人來獲取有用資訊
  - 以人性弱點瓦解組織安全
  - 利用非技術手段，獲得存取資訊或系統機會
  - 親和的聲音、假冒能力、誘人內容等是社交工程可利用之方法
  - 社交工程最具滲透力

社交工程(續)

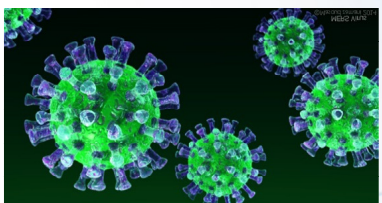
- 社交工程攻擊方式
  - 電子郵件隱藏電腦病毒
  - 釣魚網站
  - 圖片中的惡意程式
  - 偽裝修補程式
  - 即時通也是社交工程新途徑



E-mail信件潛藏危機

- 使用電子郵件信箱時，開啟來路不明郵件，可能造成電腦中毒；或輕信郵件的真實性，而讓駭客有機可乘，發動「社交工程」攻擊，造成財務損失；若您的電腦中毒了，可能導致您的電子郵件帳密被竊取。

使用者
點擊來路不明的郵件



電腦中毒/
電子郵件帳密被竊取

E-mail信件潛藏危機

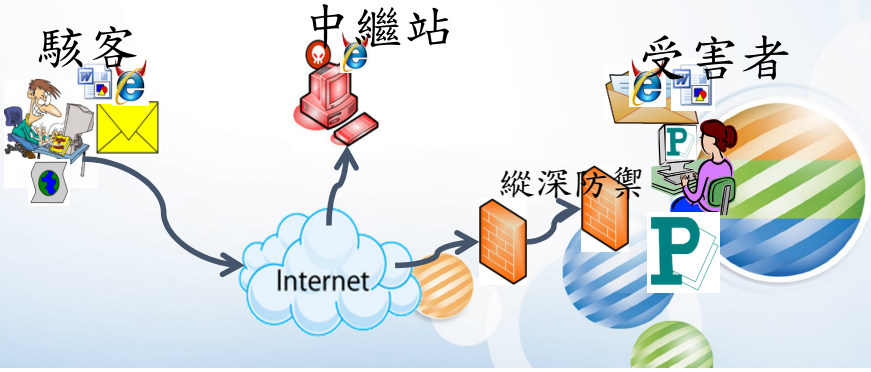
- 若您的電腦中毒了或電子郵件信箱帳密被竊取，請記得安裝防毒軟體並更新病毒碼至最新版本，對可疑的檔案進行掃描與刪除，並重新開機，若可登入信箱，強烈建議立即變更為較複雜之密碼；
- 若無法登陸信箱，則聯繫網管或郵件供應者，請其協助回復帳號。
- 最後需要檢查郵件信箱的設定，及確認郵件簽名檔中有沒有被加入惡意連結，並通知相關人，告知您的帳號被駭（盜），提醒他們多加留意，以免受騙。

《APT 攻擊駭客攻擊手法模擬》原來駭客就是這樣跟我一起上班的!!

資料來源：趨勢科技 TrendMicro

電子郵件社交工程

- 電子郵件社交工程
  - 一種攻擊行為，攻擊者利用人際關係間的互動特性所發展出來的攻擊手法
  - 一種利用人性弱點的詐騙技術，它避開了嚴密的資通安全技術防護，是一種非常難以防範的攻擊模式
  - 唯有具備高度的危機意識及警覺心，才能減少社交工程攻擊傷害



電子郵件社交工程(續)

- 如可防範社交攻擊
  - 認識常見社交工程的可疑徵兆
  - 遵守單位安全政策與程序 確認要求者的身分
  - 通報作業
- 電子郵件設定方式
  - 不自動下載圖檔
  - 關閉信件預覽功能
  - 以純文字開啟信件

行動裝置安全風險

■什麼是行動裝置？

➢電子元件在經歷數代的改進，體積已經越來越小。電腦已經普及在各式各樣的行動裝置之中。行動裝置源於個人數位助理器(Personal Digital Assistant, PDA)，以電子商用記事本為定位。行動裝置的功能越來越強大，由於攜帶方便，又結合了各種娛樂、商務功能，再加上價格也越來越便宜，現在已經普及到幾乎人手一台的地步。

➢行政院國家發展委員會

- ✓ 104年修訂「行政院及所屬各機關行動化服務發展作業原則」之智慧型行動裝置定義如下：
- ✓ **智慧型行動裝置**係指具可移動性、無線上網功能、允許使用者自行連網下載安裝應用軟體並可透過觸控面板進行操作等特性之個人化裝置，主要為智慧型手機或平板電腦。

行動裝置安全風險

■**Android存在與PNG相關漏洞**

➢Google於2019/2釋出的Android安全更新中，修補3個涉及PNG檔案的重大漏洞，相關漏洞允許駭客在PNG檔案中植入惡意程式，用戶只要點擊PNG圖片就可能觸發漏洞，導致遠端程式攻擊。PNG檔案的全名為Portable Network Graphics，專為網路傳輸所設計的檔案格式，並準備用來取代GIF。根據Google的說明，本次更新最嚴重的安全漏洞藏匿在Android框架(Framework)中，允許遠端駭客透過特製的PNG檔案，在裝置上執行任意程式，包括CVE-2019-1986、CVE-2019-1987及CVE-2019-1988，波及從Android 7.0到Android 9的各種Android版本。這代表Android用戶只要點選可愛的貓、狗圖片，或是看起來無害的風景照，都可能遭到遠端程式攻擊。

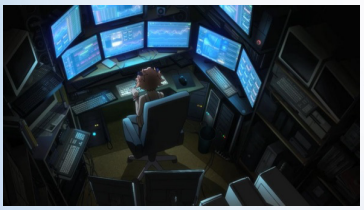
行動裝置安全風險

- 儘管Google宣稱尚未發現駭客的攻擊行動，而且已將修補版本釋出至Android開源專案(Android Open Source Project, AOSP)，但目前只有如Pixel等Google品牌的裝置可直接取得Google安全更新，至於其它品牌的手機或平板則仍得視裝置製造商或電信業者的更新時程才能取得修補，意謂仍有眾多的Android裝置陷於此一重大資安風險中。

行動裝置安全風險

■網頁挖礦程式的防範

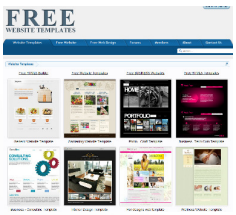
- 近年來，虛擬貨幣興起，像是比特幣、以太幣等，越來越多人投入挖礦熱潮，駭客則利用某些網站存在漏洞，將挖礦程式植入網站中，造成使用者在瀏覽該網站時，駭客則可以利用使用者的系統資源進行挖礦，使用者的系統效能則可能異常降低。



駭客

植入

挖礦程式



有漏洞的網頁

瀏覽網頁

使用者協助
系統效能異常降低

駭客可以利用使用者系統資源進行挖礦，賺取虛擬貨幣。

行動裝置安全風險

■**網頁挖礦程式的防範**

- Youtube 用戶注意！看影片電腦變慢了，可能是駭客用你電腦挖礦賺外快！！
- 外電 2018/01/29 報導，駭客利用 Youtube 用戶當礦工，他們透過 Youtube 廣告服務攻擊用戶電腦，使其成為比特幣這一類的加密貨幣礦工。
- 上週 Youtube 用戶舉報，他們在觀看 Youtube 上的廣告時，他們的反病毒軟體卻啟動了。
- 這些廣告被發現內含挖礦代碼「CoinHive」，這會對電腦發動惡意攻擊，使其占用受攻擊電腦 80% 的 CPU 為匿名駭客挖礦。
- 谷歌（Google）（GOOG-US）曾說他們密切監督其廣告服務，偵測是否被埋入加密貨幣挖礦的惡意程式。

行動裝置安全風險

■**網頁挖礦程式的防範**

- 谷歌發言人表示，「我們的平台執行多層次的偵測系統，一旦有新威脅浮現就會更新，因此在不到 2 個小時內，這些廣告就被封鎖了，且這些惡意使用者已被我們快速踢出平台。」
- 反病毒程式的供應商趨勢科技（Trend Micro）曾分析這些網路攻擊，並指明遭攻擊的國家，其網站一篇文章提到，他們的系統顯示受影響的國家包括日本、法國、台灣、意大利和西班牙，並稱他們已經將發現的資料遞交給谷歌。
- 「我們偵測到 1月24日Coinhive礦工數量增加了近285%」
- 「我們在 1月18日看到導向5大惡意網域的流量增加。」
- 「在密切檢視網路流量後，我們發現這些流量來自DoubleClick廣告。」

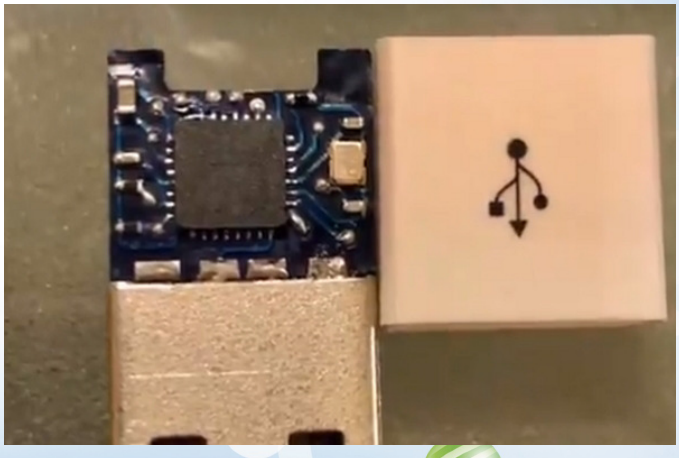
行動裝置安全風險

■**網頁挖礦程式的防範**

➢過去 12 個月加密貨幣越來越火熱，除了交易人數以外，挖礦人數也日漸增加，想要利用他人電腦為自己挖礦的駭客行動也時有所聞，用戶只能謹慎面對不知名的網域。

行動裝置安全風險

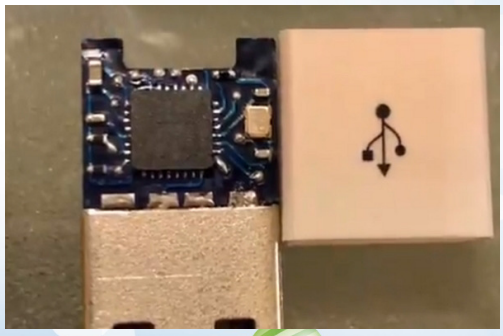
➢隨身碟除了可以儲存資料之外，對於資安有稍微瞭解的人應該知道，還可以拿來傳播病毒、或是製作一個「隨身碟炸彈」來摧毀你的PC。不過，最近又有資安人員研究出更變態的作法，他表示他靠一根USB傳輸線，就可以駭入你的硬碟並且遠端遙控你的電腦。



資料來源：https://www.ithome.com.tw/news/116175

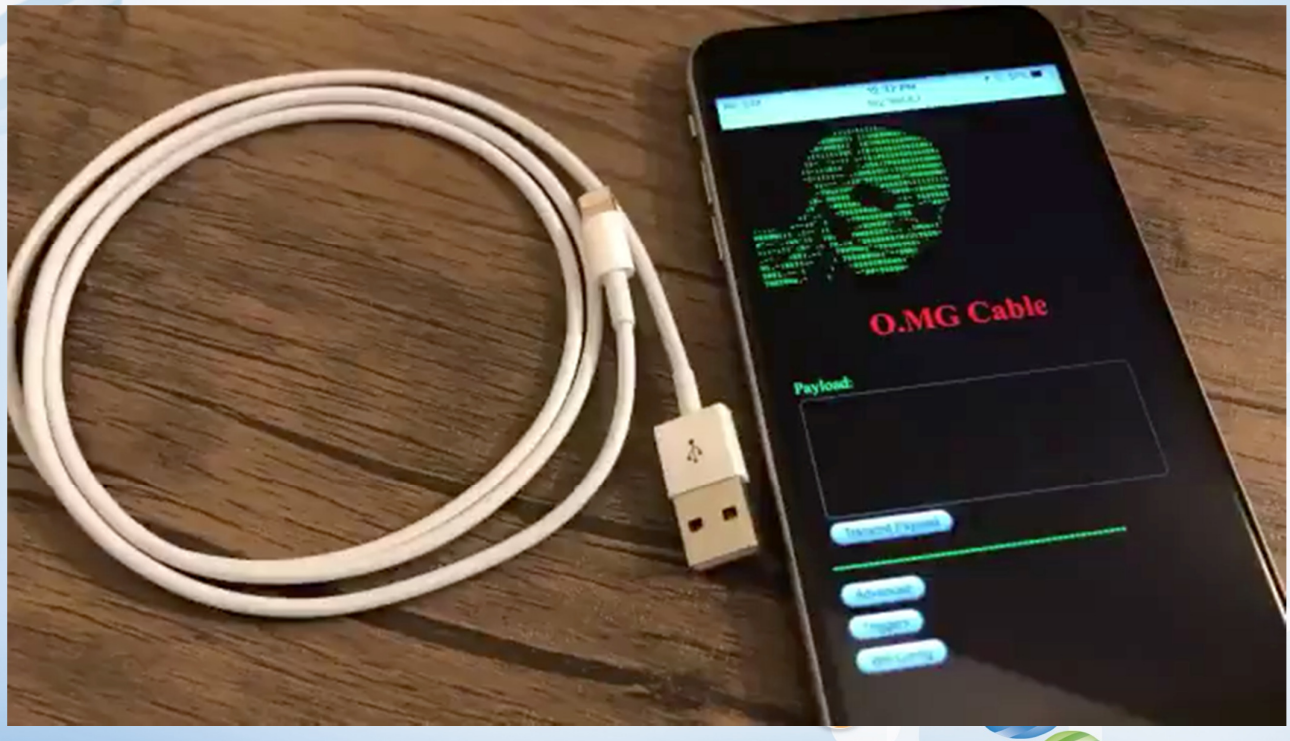
行動裝置安全風險

- 這條傳輸線稱為O.MG Cable。這樣一條內建Wi-Fi控制器的USB傳輸線，這條傳輸可以透過附近的手機來執行遠端遙控的功能，入侵到USB傳輸線插入的電腦上。
- 從外觀你完全看不出來這條傳輸線與一般傳輸線有何不同。
- O.M.G. (Offensive MG) cable可以用來控制插入的電腦，或是傳送你要受控電腦開啟的網站，甚至理論上還可以做到重刷系統韌體，你可以從這段影片來看到攻擊者透過O.MG Cable實施的攻擊過程。



資料來源：https://www.ithome.com.tw/news/116175

The OMG cable



資料來源：http://mg.lol/blog/omg-cable/

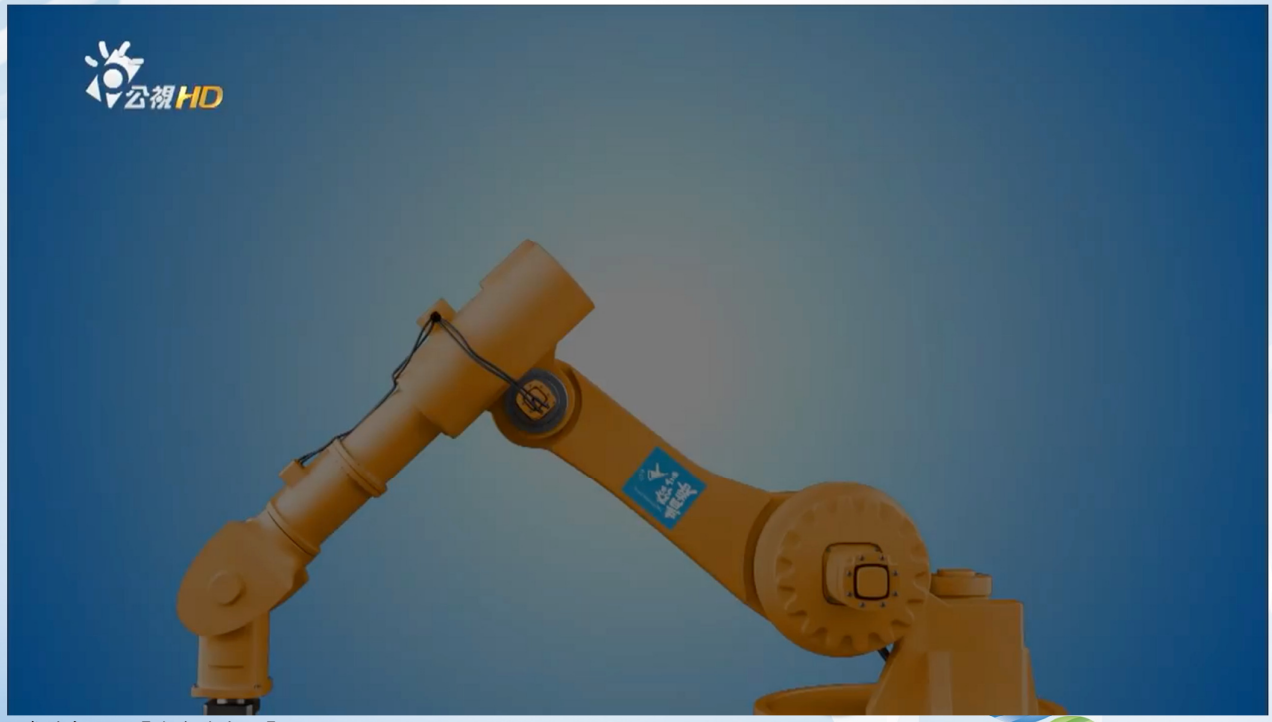
行動裝置安全風險

■2019年智慧型手機生產總量將落在14.1億支

■以全球市佔排名來看，三星(Samsung)將續擁冠軍頭銜，華為(Huawei)預估在今年超越蘋果(Apple)成為全球第二大手機品牌廠，而蘋果則將下滑一個席次至全球第三名。

資料來源： TrendForce

你的手機可能隨時都在被竊聽和監控！？



資料來源：【青春發言人】

網路消費潛藏危機

- 網路購物網站安訓安全未完善，駭客則有機會竊取您的個資，並把個資賣給詐騙集團，造成大量的詐騙案件。

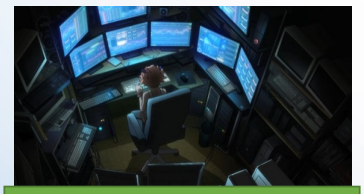
購物網站資訊安全未完善

線上購物

竊取資料

潛藏危險

詐騙、勒索



賣個資

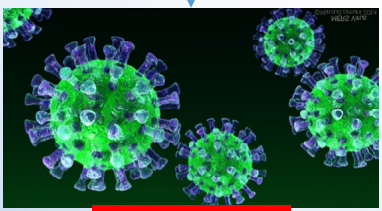
駭客透過網站漏洞入侵，竊取個資，賣給詐騙集團

網路消費潛藏危機

- 網路購物商品不實又無法退貨，消費者受詐騙，且部分網站恐潛藏惡意行為，導致消費者連網裝置遭病毒感染、資料遭竊或遭加密勒索。

線上購物

假的商品網站賣假貨的商品網站稱為一頁式詐騙



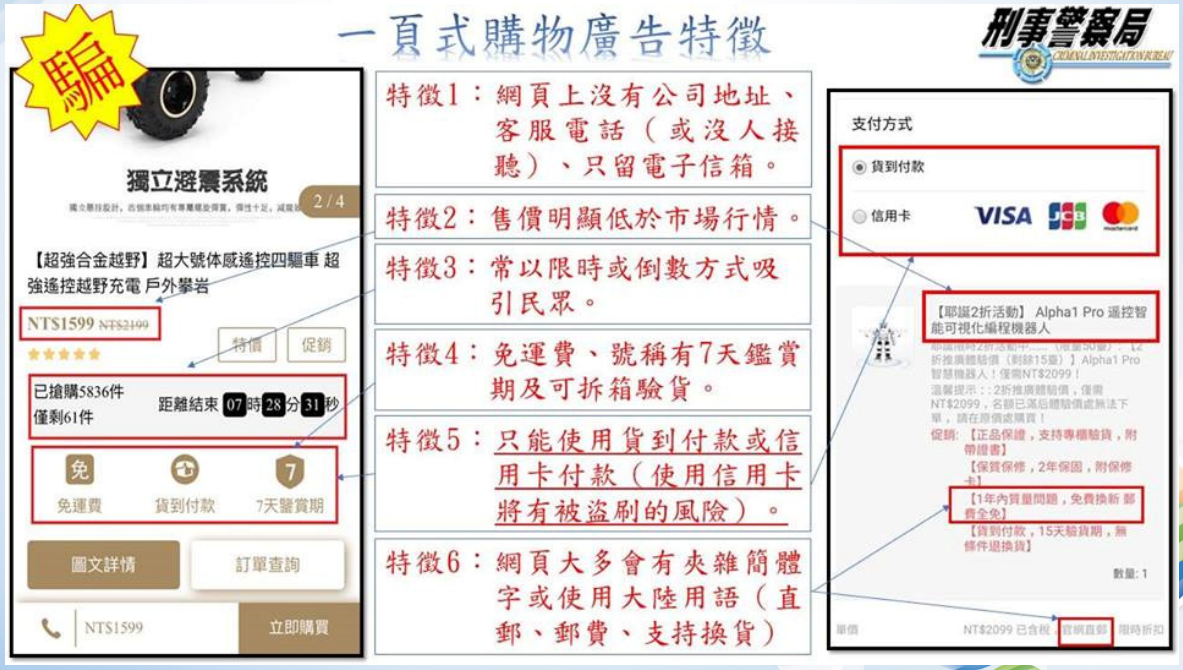
中毒

加密、勒索

消費者受騙

網路消費潛藏危機

- 一頁式詐騙網站六種特徵



資料來源：165 反詐騙

行動支付高攻擊風險 持續延燒

➢要享受行動支付帶來的便利，就應避免不安全的行為並趨吉避凶，綜合多位專家建議，使用端掌握**5**要點才能安心享受行動生活：

1. 不要破解手機取得最高權限

在**2015**年的**Black Hat**黑帽大會上，已有研究員展示可遠端竊取在**Android**手機上用戶的指紋圖像，被**root**的手機遭竊取的風險更大。指紋辨識已被用在行動錢包的身分認證上。

2. 不要安裝非官方App或在第三方平台下載App

以**Google Play**商店而言，約**0.16%**的**App**是惡意程式，但在中國大陸市場上約**13%**的**App**是惡意程式。

3. 有新版App要及時更新，以定期修補程式漏洞

資料來源：資安人 2015/12/01

行動支付高攻擊風險 持續延燒

4. 不用NFC (Near Field Communications)時就關閉此功能

日前香港傳出有2款App只要靠近NFC感應信用卡，在5秒內就可讀取持卡人姓名與個資，甚至在部分不需輸入信用卡驗證碼的網站上就可用竊來的資料盜刷。

5. 採用行動安全防護軟體

透過行動安全防護軟體可以過濾使用者安裝的App是否有安全問題，例如越來越多的越權廣告程式搜集過多使用者資訊，或將資料傳送到可疑網站，可透過安全防護軟體阻擋。

資料來源：資安人 2015/12/01

行動裝置安全風險

影片來源：https://www.youtube.com/watch?v=nsgBPTcWsY0

行動裝置安全風險

■大家都會用防毒軟體保護智慧型手機??

行動裝置安全風險

■手機會中鏢勒索病毒嗎?

- Android手機一旦不小心安裝<u>來路不明的APP</u>，<u>螢幕就會遭到鎖定</u>，然後就跳出要你付錢才能解鎖的畫面。
- iPhone手機較少案例發生，但勒索病毒會攻擊「<u>越獄</u>」（JB）過的手機。

107年資安動畫金像獎
優選：支付任意門

Chrome瀏覽器安全性設定

- **自動填入**
  - 設定 > 自動填入
- **隱私權和安全性**
  - 設定 > 進階 > 隱私權和安全性
- **重設與清理**
  - 設定 > 重設與清理

大　綱

壹 資通安全法概論

貳 資安與個資事件分享

參 社交工程與行動裝置安全管理

肆 資安事件通報規定及宣導

伍 資安政策宣導

依據

- 本辦法依資通安全管理法第14條第4項及第18條第4項規定訂定

- 明定資安事件分級
- 明定資安事件通報作業之基本通報項目

第一章 總則

第二章 公務機關資安事件通報應變

- 明定通報流程與審核作業
- 規範資安演練作業
- 明定資安事件通報規範
- 明定資安事件應變規範

配合事項

第四章 附則

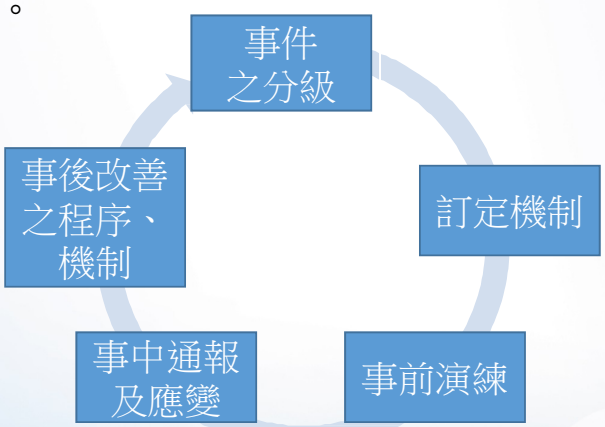
第三章 特定非公務機關資安事件通報應變

- 明定通報流程與審核作業
- 明定資安事件通報規範
- 明定資安事件應變規範

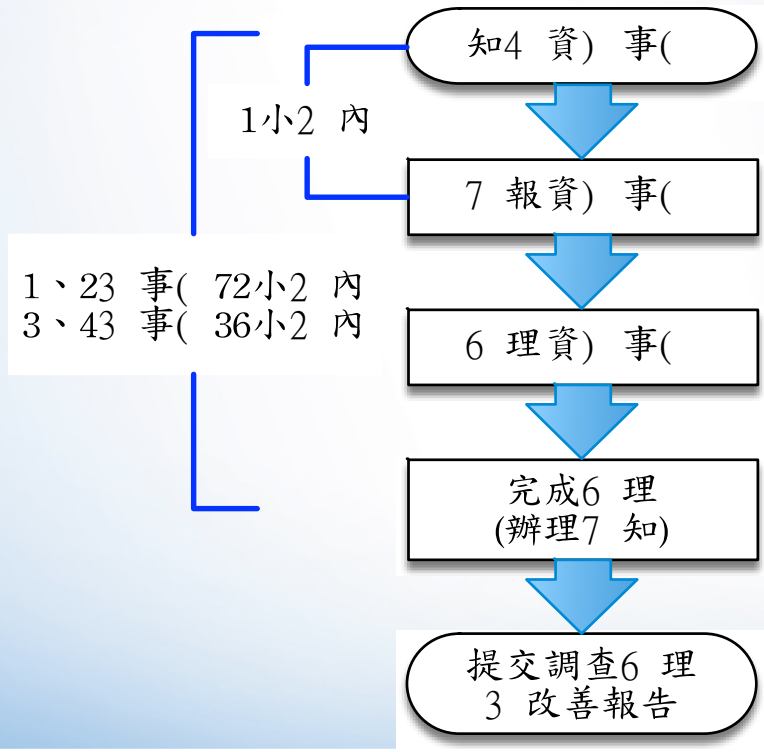
中華電信 Chunghwa Telecom

資通安全事件通報及應變辦法

- 為強化各機關之資安事件之因應。
- 規範事件之分級、訂定機制、事前演練、事中通報及應變，以及事後改善之程序、機制。



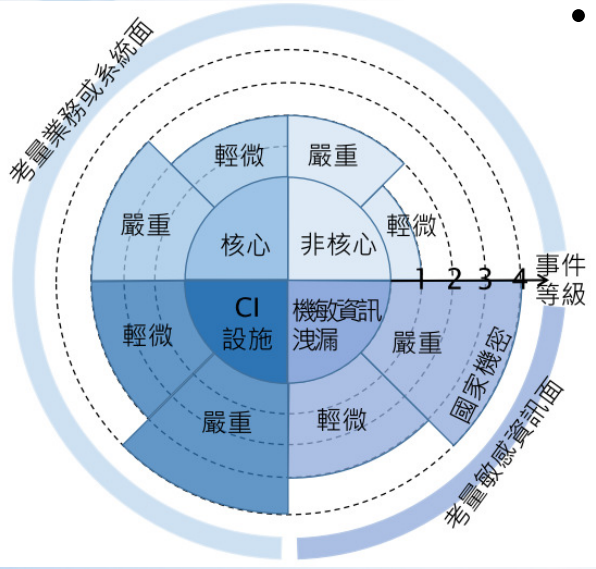
通報作業流程各項目時限



資安事件定義

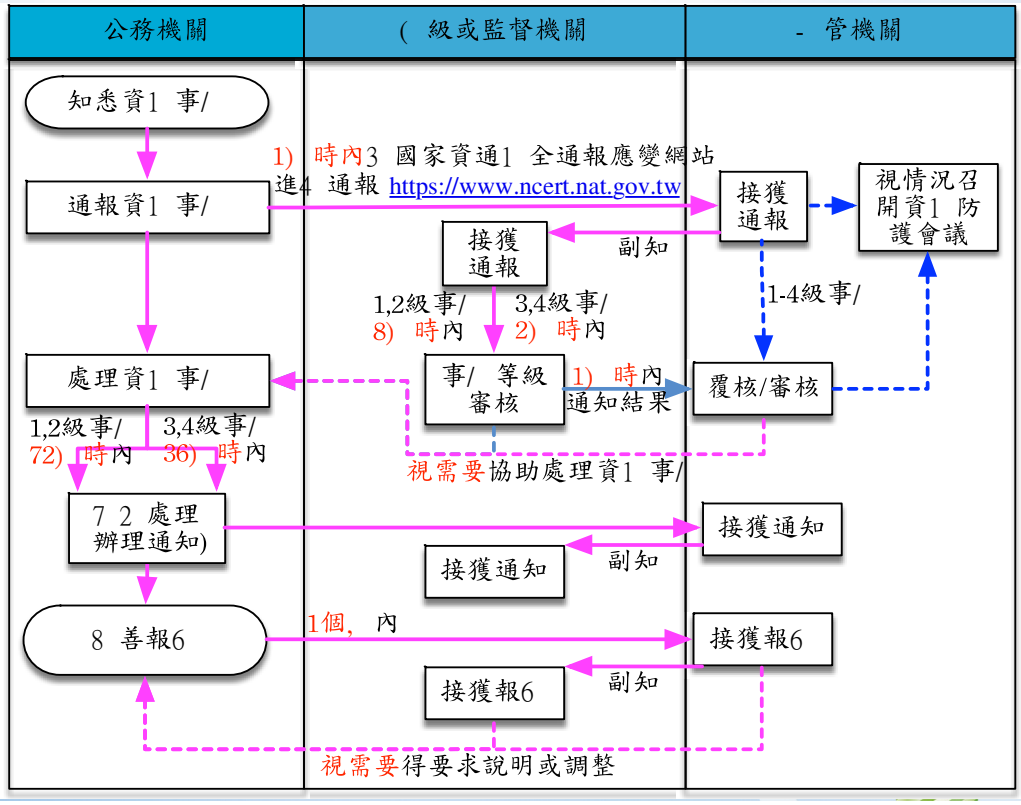
- **資通安全管理法第3條第4款**
  - 資通安全事件：指系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅。

資通安全事件分級



- 事件輕微或嚴重-考慮C、I、A
  - 機密性：
    - 業務資訊遭洩漏
  - 完整性
    - 業務資訊遭竄改
    - 資通系統遭竄改
  - 可用性
    - 資訊系統受影響或停頓，是否於可接受時間內回復

事件通報流程-公務機關



大 綱

壹 資通安全法概論

貳 資安與個資事件分享

參 社交工程與行動裝置安全管理

肆 資安事件通報規定及宣導

伍 資安政策宣導

人員對資訊安全管理系統有效性之貢獻

- 業務單位：遵守安全規定使用系統
- 稽核單位：依據規定獨立稽核是否落實執行
- 人事單位：協助資安組織與人力資源安全
- 會計單位：協助籌編預算
- 政風單位：公務機密維護
- 採購單位：第三方委外控管
- 資訊單位：建構安全的系統與環境

人員對資訊安全管理系統績效改善的益處

- 強化組織安全
- 預防性的安全管控，確保重要業務正常運作
- 建立資安危機管理及處理能力，快速處理資安事件
- 提高安全規劃效率
- 降低法律風險
- 改善與供應商的合作關係
- 持續保護

未遵循ISMS 要求事項之可能後果

公務機關所屬人員辦理資通安全業務獎懲辦法

第四條：有下列情形之一者，予以懲處：

一、未依本法 、本法授權訂定之法規或機關內部規範辦理列事項，下列事項， 情節重大 ：

(一)資通安全情分享作業。

(二)訂定、修正及實施資通安全維護計畫。

(三)提出資通安全維護計畫實施情形。

(四)辦理資通安全維護計畫實施情形之稽核。

(五)配合上級或監督機關資通安全維護計畫實施情形稽核結果，提出改善報告。

(六)訂定資通安全事件通報及應變機制。

(七)資通安全事件之通報或應變作業。

(八)提出資通安全事件調查、處理及改善報告。

未遵循ISMS 要求事項之可能後果

二、辦理資通安全業務經主管機關、上級或監督機關評定績效不良，經疏導無效，情節重大。

三、其他違反本法、本法授權訂定之法規或機關內部規範之行為，情節重大。

第五條公務機關辦理其所屬人員之平時考核，應審酌前二條所定獎勵及懲處情形，依事實發生之原因、經過、行為之動機、目的、手段、表現、所生之影響等因素為之；其所屬人員為聘用人員、約僱人員或其他與機關有僱傭關係之人員者，其獎勵及懲處之情形並應納入續聘之參考。

攜手合作 共創雙贏

中華電信

資安最佳選擇 中華電信團隊

敬請指教！