國立中科實驗高級中學

National Experimental High School at Central Taiwan Science Park

資安宣導課程教育訓練

中華民國111年05月

課程大綱

- 資訊安全政策及法令法規
- 資安重要性及資安威脅影響面
- E-mail信件潛藏危機
- 資安與個資事件分享
- 社交工程與行動裝置安全管理
- 為何需要資訊（效益）
- 未遵循 ISMS 要求事項之可能後果
- 問題與討論

資訊安全政策及法令法規

資訊安全政策

文件編號：NEHS-ISMS-A-001

版次：1.0

目的

- 為確保國立中科實驗高級中學（以下簡稱本校）所屬之資訊資產的機密性、完整性、可用性及符合相關法規之要求，導入資訊安全管理系統，強化本校資訊安全管理，保護資訊資產免於遭受內、外部蓄意或意外之威脅，維護資料、系統、設備及網路之安全，提供可靠之資訊服務，訂定本政策。

資訊安全政策

- 文件編號適用範圍：
  - 本政策適用範圍為本校之全體人員、委外服務廠商與訪客等。
  - 資訊安全管理涵蓋14項管理事項，避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、洩漏、竄改、破壞等情事發生，對本公司帶來各種可能之風險及危害。管理理事項如下：

資訊安全政策

- 資訊安全政策訂定與評估。
- 資訊安全組織。
- 人力資源安全。
- 資產管理。
- 存取控制安全。
- 密碼控制措施。
- 實體與環境安全。
- 運作安全。
- 通訊安全。
- 系統獲取、開發及維護
- 供應者關係

資訊安全政策

- 資訊安全事故管理。
- 營運持續管理的資訊安全層面管理。
- 相關法規與施行單位政策之符合性。

本公司之內部人員、委外服務廠商與訪客皆應遵守本政策。

資訊安全政策

- 目標:
  - 維護本校資訊資產與個資資產之機密性、完整性與可用性，並保障使用者資料隱私。藉由全體同仁共同努立來達成下列目標:
  - 確保相關資通安全措施或規範符合政策與現行法令的要求每年至少進行一次內部稽核。
  - 每年至少進行一次業務持續計畫之測試或檢核。

資訊安全政策

- 辦理資訊安全教育訓練，推廣資訊安全之意識與強化其對相關責任之認知。
- 符合政府資通安全相關政策、規訂及相關法令要求。

資訊安全政策

■責任：

- 本校應成立資訊安全組織統籌資訊安全事項推動。
- 管理階層應積極參與及支持資訊安全管理制度，並授權資訊安全組織透過適當的標準和程序以實施本政策。
- 本校全體人員、委外服務廠商與訪客等皆應遵守相關安全管理程序以維護本政策。
- 本校全體人員及委外服務廠商均有責任透過適當通報機制，通報資訊安全事件或弱點。
- 任何危及資訊安全之行為，將視情節輕重追究其民事、刑事及行政責任或依本校之相關規定進行議處。

資訊安全政策

■審查:

- 本政策應每年至少審查乙次，以反映政府法令、技術及業務等最新發展現況及關注方之關注議題，以確保本校資訊安全管理制度之運作。

■實施:

➢本政策經「資訊安全委員會」進行審核後實施，修訂時亦同。

相關法令法規

- 資通安全管理法
- 資通安全管理法施行細則
- 資通安全責任等級分級辦法
- 資通安全事件通報及應變辦法
- 資通安全情資分享辦法
- 公務機關所屬人員資通安全事項獎懲辦法
- 資訊系統風險評鑑參考指引
- 政府資訊作業委外安全參考指引
- 無線網路安全參考指引
- 網路架構規劃參考指引
- 行政裝置資安防護參考指引
- 政府行動化安全防護規劃報告
- 資訊作業委外安全參考指引

資訊安全重要性及威脅影響面

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。

資安重要性及資安威脅影響面

資安威脅影響層面

國家	企業	個人
關鍵資訊及	經濟損失	檔案勒索
基礎設施遭駭	商譽受損	財務盜刷
引發政經民心動亂	機密外洩	個資外洩
	喪失競爭力	遭受詐騙

資安三不政策，五項口訣

三不政策	五項口訣
不點擊可疑網頁/郵件連結	系統弱點要修補
不任意開啟郵件附檔	資安訓練要確實
不安裝來源不明軟體	掃毒作業要執行
	資安新聞要專注
	遇可疑立即反應


X1
=
$10000
qoogle Pet
但是挺貴的

資安重要性及資安威脅影響面

美國海關外包商系統遭駭客入侵

- 美國海關暨邊境保衛局(U.S. Customs and Borders Protection, CBP)於6/10發布聲明指出，其委外廠商於5/31遭遇「重大惡意網路攻擊」導致資料外洩，但目前還未見到有任何資料或照片流至網際網路或暗網上。CBP表示，該委外廠商在違反規定與未知會取得海關授權情況下，將系統蒐集的旅客相片或車牌相片檔複本，逕行傳送到其公司網路上。委外廠商內部網路在一次惡意網路攻擊下被入侵，因而導致這起資料外洩事件。CBP已經將與此次事件有關的所有設備移除，通知國會與警方，並嚴密監控中。CBP表示其本身系統並未受影響，但不願說明有多少資料被竊、攻擊事件規模、或是有多少美國公民受影響，也不願透露委外廠商的名稱。

資料來源：https://www.nccst.nat.gov.tw/ 2019/06/17

資安重要性及資安威脅影響面

臺灣已是連續六年遭受假消息攻擊最嚴重的國家

- 根據大型民主指標研究Varieties of Democracy的資料，臺灣自2013年來，受到外國假消息攻擊的情形就已經是全球第一嚴重，並有更趨嚴重的趨勢，至於政府對國外傳播假消息方面，則是委內瑞拉為第一嚴重的國家。
- 近年來，假消息被國家操控的威脅，在國際上成為議論焦點，像是2016美國總統大選時就有借鑑，而這樣的議題近期也在臺灣發酵。
- 最近，政治學界所關注的大型民主指標研究Varieties of Democracy（V-Dem），在4月8日釋出的第9版資料庫，也有假消息與政府相關的量化數據，並且其中的調查結果顯示了臺灣的嚴重性，因此被許多人引用。但是，資料庫當中其實還包括了不同假消息流向的分析，不只是境外對國內，還有像是政府對國外傳播假消息，或是政府對國內本身傳播假消息，同樣值得關注。

資料來源： https://www.ithome.com.tw/news/129922 2019/04/11

資安重要性及資安威脅影響面

臺灣已是連續六年遭受假消息攻擊最嚴重的國家

- 根據大型民主指標研究Varieties of Democracy的資料，臺灣自2013年來，受到外國假消息攻擊的情形就已經是全球第一嚴重，並有更趨嚴重的趨勢，至於政府對國外傳播假消息方面，則是委內瑞拉為第一嚴重的國家。
- 近年來，假消息被國家操控的威脅，在國際上成為議論焦點，像是2016美國總統大選時就有借鑑，而這樣的議題近期也在臺灣發酵。
- 最近，政治學界所關注的大型民主指標研究Varieties of Democracy（V-Dem），在4月8日釋出的第9版資料庫，也有假消息與政府相關的量化數據，並且其中的調查結果顯示了臺灣的嚴重性，因此被許多人引用。但是，資料庫當中其實還包括了不同假消息流向的分析，不只是境外對國內，還有像是政府對國外傳播假消息，或是政府對國內本身傳播假消息，同樣值得關注。

資料來源： https://www.ithome.com.tw 2019/04/11

資安重要性及資安威脅影響面

行政院發布「危害國家資安產品限制原則」將不僅限於中國商品

- （中央社）行政院19日發布「各機關對危害國家資通安全產品限制使用原則」，要求各機關除因業務需求且無其他替代方案外，不得採購及使用危害國家資通安全的廠商產品；經各相關機關盤點後，最快3個月後以正面表列方式公布清單。
- 對於原則的內容沒有涵蓋中國字眼，行政院發言人Kolas Yotaka（谷辣斯．尤達卡）解釋，在討論過程中發現，有疑慮的商品未必只來自中國，還有其他國家，因此在原則中未特定指涉某一個國家；不過，來自中國的產品是在約束範圍內。

資料來源：中央社 2019/04/20

資安重要性及資安威脅影響面

行政院發布「危害國家資安產品限制原則」將不僅限於中國商品

- 政院官員表示，華為、中興通訊、聯想電腦、海康威視等中國品牌，未來不排除納入禁止使用清單中。
- 資通安全即國安，經過數月研議討論，行政院長蘇貞昌18日核定「各機關對危害國家資通安全產品限制使用原則」，政院隨即發文中央各部會與各地方政府，使用原則「已經生效」。Kolas也召開記者會對外說明。
- 根據處理原則，各機關盤點後若發現有資安疑慮的產品：
  - 應指定特定區域及特定人員使用。
  - 不得與公務網路環境介接。
  - 不得處理或儲存機關公務資訊。
  - 測試或檢驗結果應產出報告。
  - 購置理由消失，或使用年限屆滿應立即銷毀。

資料來源：中央社 2019/04/20

資安重要性及資安威脅影響面

行政院發布「危害國家資安產品限制原則」將不僅限於中國商品

- 不過，Kolas說，這項處理原則不適用「個人消費」與「民間採購」，僅針對中央政府機關（行政院與所屬各部會）、地方政府、公營事業及行政法人、公立學校，以及關鍵基礎設施提供者和政府捐助的財團法人（例如工研院、資策會）。
- 其中，關鍵基礎設施包含8大類。Kolas表示，關鍵基礎設施提供者與政府捐助的財團法人，將由目的事業主管機關（例如金管會、NCC與科技部、經濟部、衛福部等）進行督導與要求。
- 此外，對資通產品的定義，Kolas表示，包括伺服主機、網路攝影機、無人機、雲端服務、電信業的核心骨幹網絡設備、電腦軟體、防毒軟體、機關委外開發的系統、委外通訊顧問，或是委外請企業規劃、開發系統等。

資料來源：中央社 2019/04/20

資安重要性及資安威脅影響面

行政院發布「危害國家資安產品限制原則」將不僅限於中國商品

- 她說，「各機關對危害國家資通安全產品限制使用原則」適用機關在採購上述資通產品時，均必須符合處理原則；希望地方政府，不分藍綠，共同遵守這項原則，因為政府是一體的，重要資訊會在中央與地方政府流通，中央與地方政府共同維護國安。
- Kolas強調，這項處理原則核定後，各機關要針對現在使用或所採購的產品進行盤點，找出是否有來自危險地區的商品，3個月內，把有疑慮的品牌與商品提給中央，再由中央彙整清單。
- 行政院完成彙整後，估計最快3個月後可公布，屆時會用正面表列方式列出有疑慮的品牌與產品。同時，行政院可能採用具有法律效力的形式，以約束相關機關構，避免採購有資安疑慮的產品。

資料來源：中央社 2019/04/20

資安重要性及資安威脅影響面

行政院發布「危害國家資安產品限制原則」將不僅限於中國商品

- Kolas也進一步解釋，之所以要訂定這項採購原則，主要是因去年底總統府國安會分別在12月14日與12月26日，就資通產品採購召開二次專案會議，國安會方面希望行政院可以依據《資通安全管理法》訂定一個管理機制。原本是預計1月和3月底完成處理原則之制定，但討論過程認為應該更周延，因此一直到18日才完成採購原則的公告程序。

資料來源：中央社 2019/04/20

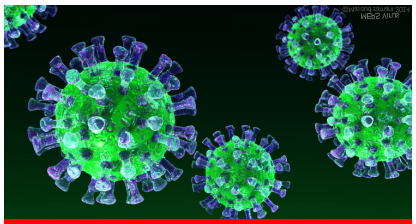
E-mail信件潛藏危機


twcertcc
台灣電腦網路危機處理暨協調中心
Taiwan Computer Emergency Response Team / Coordination Center
網路釣魚防詐資安宣導

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。

資訊安全與個資事件分享

資訊安全
與
個資事件分享

學生研究漏洞惹禍！臺灣大學CEIBA教學平臺成績全部變成87分，目前已恢復最近5學年資料

臺灣大學的課程管理平臺CEIBA疑似遭到攻擊，所有學生的成績都被改成87分，事隔2天校方才證實，這是資工系學生執行滲透測試造成的烏龍攻擊事件

文/ 周峻佑 | 2019-11-10 發表

讚 250 分享

臺灣大學 National Taiwan University 校園公佈欄

回上一頁

公告主旨	CEIBA 成績資料修復中
公告單位	教務處--教學發展中心教學科技組
公告時間	2019/11/6 上午 09:00:31 0 LIKE 0 DISLIKE
	各位老師、各位同學大家好 由於 CEIBA 資料庫資料異常，目前正緊急進行更正作業。

圖片來源: 臺灣大學

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

資訊安全
與
個資事件分享

注意：玩手遊也會中獎

- 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，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 商店中被感染的式，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。

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

資訊安全
與
個資事件分享

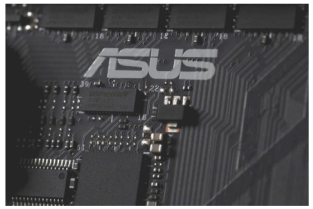
NASA伺服器遭駭客入侵

- 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，受到影響的是身分為公務員(NASA Civil Service)的員工，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/

資訊安全
與
個資事件分享

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

資訊安全
與
個資事件分享

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

資訊安全
與
個資事件分享

中山大學驚傳師生電子郵件被監控長達3年，起因是駭客濫用Open WebMail漏洞，其他學校也應留意相關系統安全

採用Open WebMail建置電子郵件系統的單位要注意了！最近中山大學坦承，他們的電子郵件信箱遭到入侵逾3年，駭客監控近百人的信件，其中大部分是社會學系的教授

文/ 周峻佑 | 2019-11-08 發表

讚 502 分享

圖片來源: 中山大學

資訊安全
與
個資事件分享

猶他大學遭勒索軟體攻擊：付贖金的原因不是為了解密資料，而是贖回被盜的學生資料

校方雖然有能力復原被勒索軟體加密的系統，但礙於駭客同時也取走教職員與學生檔案，為避免個資外流，仍選擇支付贖金給駭客

文/ 陳曉莉 | 2020-08-21 發表

讚 331 分享

Photo by University of Utah on https://twitter.com/UUtah/status/1290772408996171777/photo/1

這兩年有愈來愈多的勒索軟體駭客集團在加密系統上的資料前，會先下載資料，以增加與被害者談判的籌碼，而本周美國猶他大學即證實了這個現況。猶他大學以一己之力復原了被駭客加密的系統，卻為了保護被


個人資料保密

社交工程與行動裝置安全管理

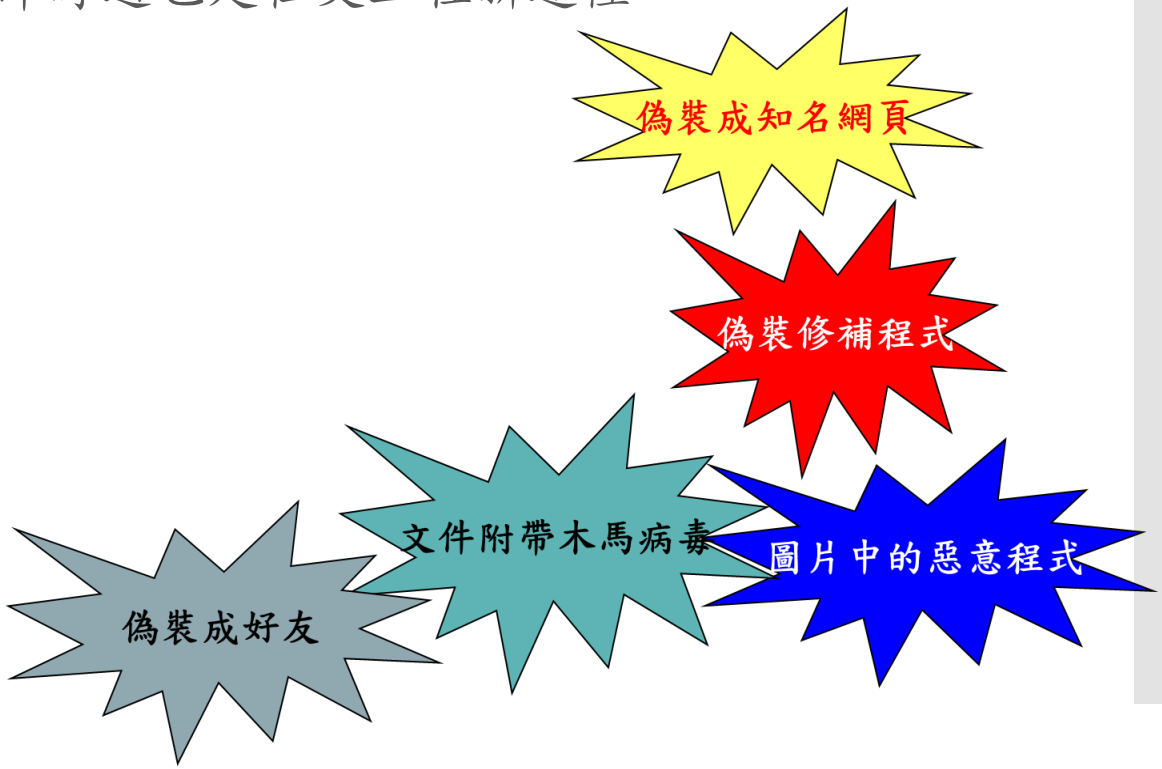
社交工程
與
行動裝置安全
管理

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

社交工程與行動裝置安全管理

- 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

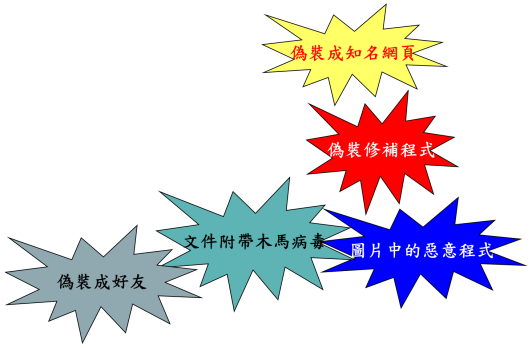


社交工程
與
行動裝置安全
管理

常見的社交工程攻擊方式有哪些?
應如何防範?

社交工程（Social Engineering）係利用人性弱點，應用簡單的溝通和欺騙技倆，以獲取帳號、通行碼、身分證號碼或其他機敏資料，來突破組織的資通安全防護，遂行其非法的存取、破壞行為。

- 常見的社交工程攻擊方式如下：
  - 電話詐騙
    - 利用電話佯裝資訊人員，騙取帳號及通行碼。
    - 偽裝委外廠商之維護人員或上級單位人員，乘機騙取帳號及通行碼。



資料來源：資通安全處 2013/10/24

社交工程
與
行動裝置安全
管理

常見的社交工程攻擊方式有哪些?
應如何防範?

- 常見的社交工程攻擊方式如下：
  - 電子郵件詐騙
    - 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
    - 利用電子郵件誘騙使用者登入偽裝之網站以騙取帳號及通行碼，如網路釣魚。
    - 利用電子郵件誘騙使用者開啟檔案、圖片，以植入惡意程式、暗中收集機敏性資料。

資料來源：資通安全處 2013/10/24

社交工程
與
行動裝置安全
管理

常見的社交工程攻擊方式有哪些?
應如何防範?

- 常見的社交工程攻擊方式如下：
  - 網路釣魚
    - 利用電子郵件誘騙使用者登入偽裝之網站以騙取帳號及通行碼，如網路釣魚。
  - 圖片內含惡意程式
    - 利用電子郵件、通訊軟體等誘騙使用者開啟檔案、圖片，以植入惡意程式、暗中收集機敏性資料。
  - 偽裝修補程式
    - 利用提供工具、檔案、圖片為幌子，誘騙使用者下載，如偽裝的修補程式 、 p2p 下載軟體、工具軟體等，乘機植入惡意程式、暗中收集機敏性資料。

資料來源：資通安全處 2013/10/24

社交工程
與
行動裝置安全
管理

常見的社交工程攻擊方式有哪些?

- 常見的社交工程攻擊方式如下：
  - IM, Line, MSN, Yahoo, Skype...
    - 利用即時通訊軟體如 MSN ，偽裝親友來訊，誘騙點選來訊中之連結後中毒。

社交工程雖然利用人性弱點來騙取機敏資料，讓人覺得防不勝防，但如果能隨時提高警覺，不未經確認即提供資料、不開啟來路不明的電子郵件及附加檔案、不連結及登入未經確認的網站、不下載非法軟體及檔案，就能避免社交工程的攻擊傷害。

資料來源：資通安全處 2013/10/24

社交工程
與
行動裝置安全
管理

應如何防範社交工程?

- **正確地使用電子郵件**
  - ✓不自動下載圖檔。
  - ✓關閉郵件預覽功能。
  - ✓以純文字開啟信件。
  - ✓除非相當確定信件的來源，否則決不輕易開啟或點擊信件裡的附件檔案或超連結。
  - ✓不要將電子郵件密碼告知任何人，即使是系統管理者。
  - ✓不要使用電子郵件傳輸任何不當資訊，包括不法、暴力、色情、違法交易、侵犯隱私或威脅他人的資料。
  - ✓非公務郵件轉寄前先將他人郵件地址刪除，避免他人郵件地址傳出。
  - ✓非公務郵件同時寄件給多人時，為保護各收信人資訊，最好使用「密件副本」方式傳送。
  - ✓不要將電子郵件帳號轉借他人使用。
  - ✓不要轉寄不明網路謠言及發送廣告信。

社交工程
與
行動裝置安全
管理

應如何防範社交工程?

- **社交工程的基本防護**
  - ✓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
  - ✓執行各種作業系統、應用軟體的更新及設定。
  - ✓必須安裝防毒軟體，並確實更新病毒碼。
  - ✓密碼設定要符合複雜度的要求。
  - ✓不要輕易相信電話中任何非經正式授權的請求。
  - ✓不於社群網路中談論有關公務之相關內容。
  - ✓修改個人資料的隱私設定(提供最少個資為宜)。
  - ✓不要輕易點選陌生的加好友請求。
  - ✓不任意點選社群網路聊天室或電子郵件的連結。
  - ✓不要任意安裝未經授權的軟體。
  - ✓小心釣魚網站、詐騙廣告的陷阱。
  - ✓不使用公務信箱作為登入的帳號。

社交工程
與
行動裝置安全
管理

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。

社交工程
與
行動裝置安全
管理

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。

社交工程
與
行動裝置安全
管理

行動裝置安全風險

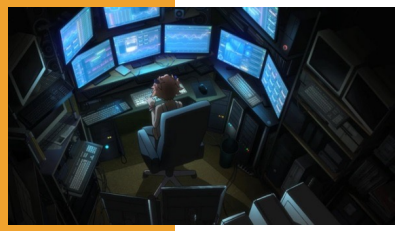
- 儘管Google宣稱尚未發現駭客的攻擊行動，而且已將修補版本釋出至Android開源專案(Android Open Source Project, AOSP)，但目前只有如Pixel等Google品牌的裝置可直接取得Google安全更新，至於其它品牌的手機或平板則仍得視裝置製造商或電信業者的更新時程才能取得修補，意謂仍有眾多的Android裝置陷於此一重大資安風險中。

社交工程
與
行動裝置安全
管理

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。

社交工程
與
行動裝置安全
管理

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。

社交工程
與
行動裝置安全
管理

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。」

社交工程
與
行動裝置安全
管理

行動裝置安全風險

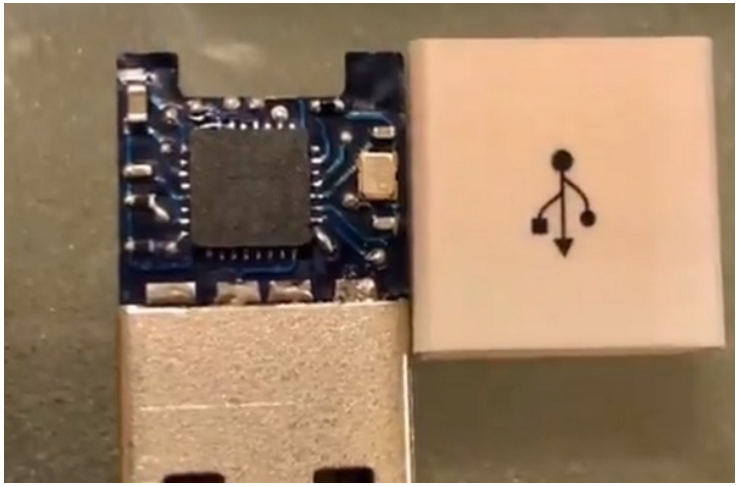
■ **網頁挖礦程式的防範**

➢ 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。

社交工程
與
行動裝置安全
管理

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。

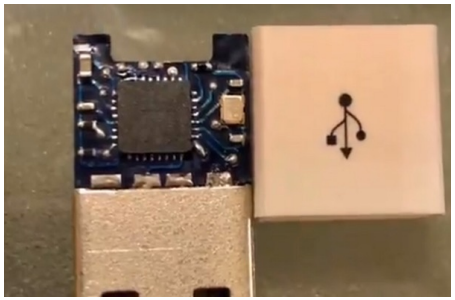


資料來源:
https://www.ithome.com.tw/news/116175

社交工程
與
行動裝置安全
管理

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

社交工程
與
行動裝置安全
管理

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

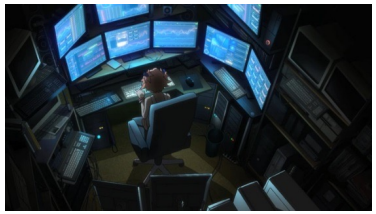
社交工程
與
行動裝置安全
管理

網路消費潛藏危機

- 網路購物網站資訊安全安全未完善，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

竊取資料



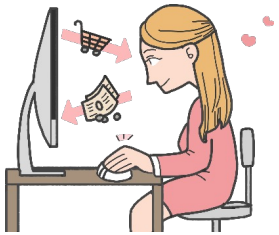
駭客透過網站漏洞入侵，竊取個資，賣給詐騙集團

線上購物

潛藏危險

賣個資

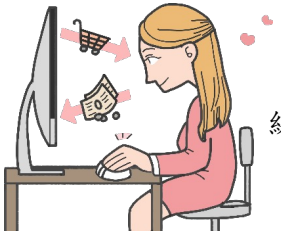
詐騙、勒索



社交工程
與
行動裝置安全
管理

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

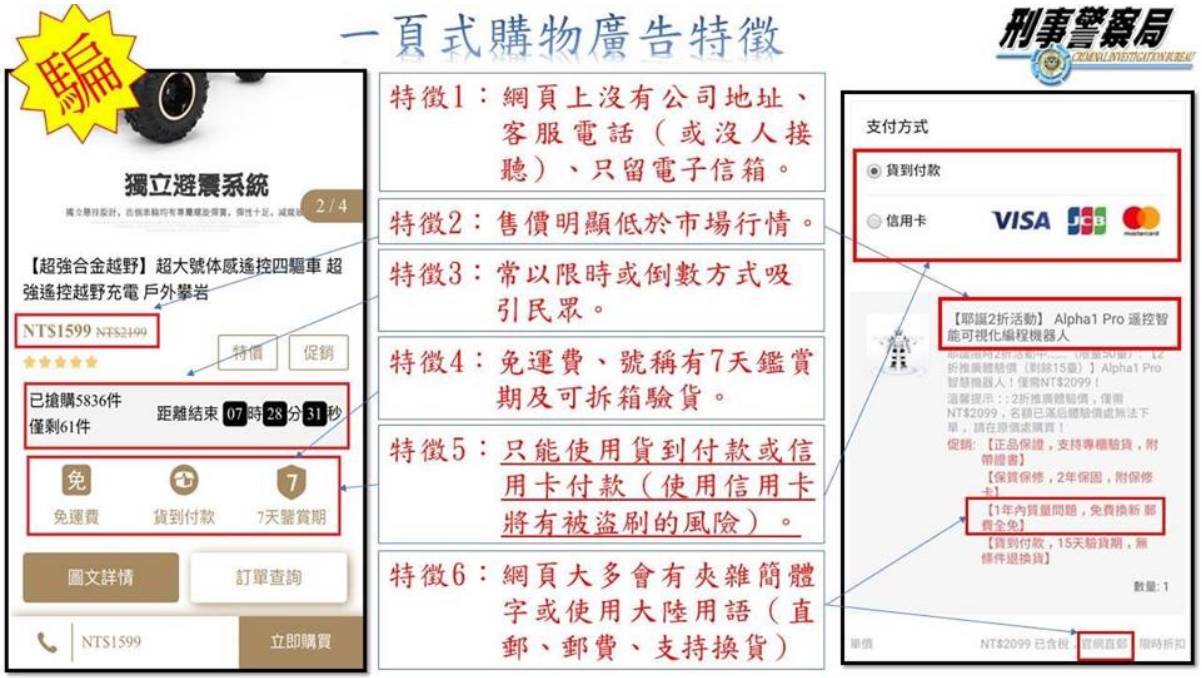
中毒

加密、勒索

消費者受騙

社交工程與行動裝置安全管理

- 一頁式詐騙網站六種特徵



資料來源：165 反詐騙

社交工程
與
行動裝置安全
管理

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

社交工程
與
行動裝置安全
管理

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

社交工程與行動裝置安全管理

- 大家都會用防毒軟體保護智慧型手機??

社交工程與行動裝置安全管理

■手機會中鏍勒索病毒嗎？

- Android手機一旦不小心安裝來路不明的APP，螢幕就會遭到鎖定，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「越獄」（JB）過的手機。

為何需要資訊（效益）

為何需要資訊（效益）

- 業務持續重要性與安全目標
  - 資訊安全是為了保護組織的資訊安全，而資訊安全的目標是設定組織內如何可以持續運作的資安管理目標與相關機制。
  - 資訊安全的定義是考量如何維持資訊的機密性、完整性及可用性；同時可以包括鑑別性、可歸責性、不可否認性及可靠性等方向。

未遵循 ISMS 要求事項之可能後果

未遵循 ISMS 要求事項之可能後果

未遵循資訊安全管理系統要求事項之可能後果

- 造成資安事件、事故（含機密外洩）。
- 造成個資事件、事故（含個資外洩）。
- 造成顧客損失。
- 造成本校損失。
- 遭受相關法令起訴。
- 造成個人損失。

問題與討論

沒有百分之百的資訊安全，

得靠每個人從小地方一起努力！

感謝聆聽