網路應用與安全

丁德榮

簡歷

- 新竹師專 、文化資科、交大資科畢業
- 國小教師 6年(萬里、五常)
- 國中教師 4年(順天、北勢)
- 高職教師 4.5年(新力工家、嶺東工商、沙鹿高工)
- 弘光科大 2年(資管系助理教授兼電算中心主任)
- 彰化師範大學 資訊工程系 11年
- 現職 彰化師範大學 資訊工程系

大綱

- 網路應用
  - 社群網站、網路購物、物聯網、NFC應用
- 網路安全
  - 網路安全簡介
  - 密碼學簡介
  - 網路安全應用
  - 網路安全實例與防範
  - Facebook安全
  - 手機安全
- 結語

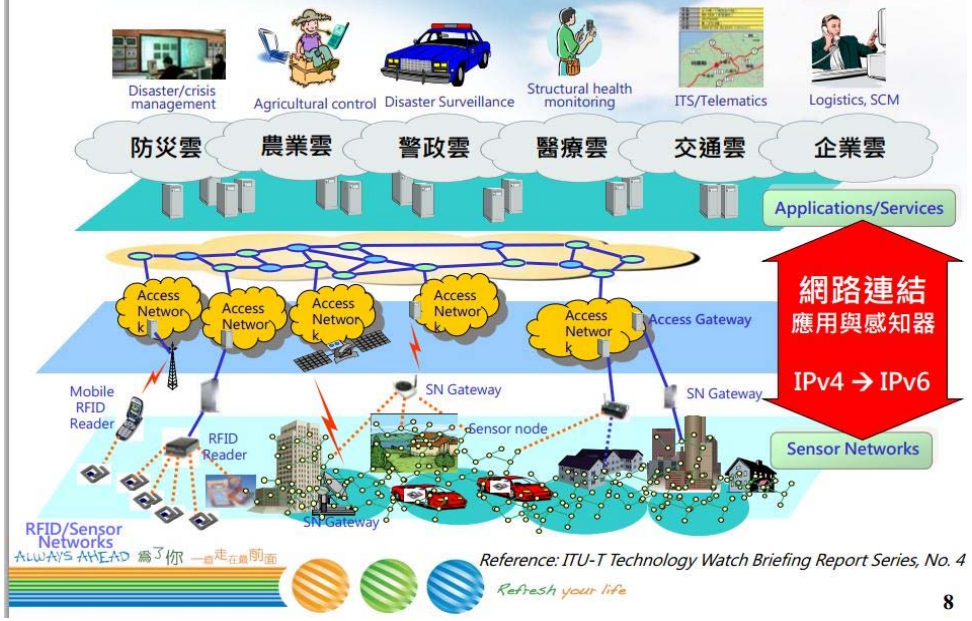
社群網站 :Facebook(FB), Twitter(推特), Plurk(撲浪), Line

- 封閉式社交社群
- 關連式與探勘服務
- 個人人脈使用

網路購物

物聯網發展議題 - 網路架構

中華電信 Chunghwa Telecom



Reference: ITU-T Technology Watch Briefing Report Series, No. 4

智慧生活

NFC(Near Field Communication)稱為近場通訊 (或稱為近距離無線通訊)

NFC Historic Sites

- Nearby
- Sharing

台灣的NFC服務

- 中華電信、悠遊卡公司、恩智浦半導體(NXP)與萬事達卡PayPass合作於2011/12/8推出服務
- 「悠遊卡 NFC 背夾」PayPass 版需與玉山銀行、台新銀行、國泰世華銀行申辦，就能在接受萬事達卡 PayPass 服務的商家進行刷卡付費。

紐約地鐵NFC虛擬圖書館

- 邁阿密廣告學院的學生設置
- NFC 手機掃描一下可以閱讀書的前10頁
- 出地鐵後此書的實體資訊會傳送到手機的地圖上，有興趣可租借回家閱讀

為何要使用手機便利付?

手機付費趨勢

- 智慧型手機持有用戶數：約1,200萬(51%)
- 無線上網人數：1,107萬(其中行動上網為854萬人)
- 目前的**收費機制**
  - **信用卡綁定App商城金流**
  - **遊戲點數卡：MyCard, Gash, 元氣卡,辣椒卡...**
  - **電信運營商小額付費**
  - **第三方交易付費機制(PayPal)**

個資外洩事件

- 包括波音、美國退伍軍人事務部、惠普公司（HP）、McAfee、加州大學，誠品網路書局、東森購物等。
- SONY, APPLE, PayEasy受「駭」 5400會員個資外洩
- 博客來個資外洩事件
- 大考中心
- 網路選課

資訊安全與網路安全簡介

網路安全是什麼?

- 網路安全:
  - 保護資料安全
  - 保護資料與網路傳送的安全

網路安全的目標

- **機密性 Confidentiality**
  - 未經授權之人無法存取資料
  - 避免故意或無心而未經授權竊取及洩漏資料內容
- **完整性或真確性 Integrity**
  - 確保資產之正確性與完整性之性質
  - 未經授權之人員或程序無法竄改資料
  - 經授權之人員或程序無法執行未獲授權之修改
  - 資料之內外一致
- **可用性 Availability**
  - 確保有需要時，系統能上線或執行
  - 未經授權之人無法阻撓合法用戶使用系統資源
  - 經授權人員可及時可靠地存取資料或電腦資源

網路安全的重點

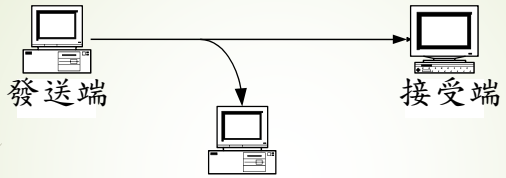
- **不可否認性**
  - 來源端不可否認性
  - 接收端不可否認性
- **認證(authentication)與數位簽章(digital signature)**
  - 辨別傳送訊息者之身分
- **存取控制**
- **稽核**

資訊安全的威脅

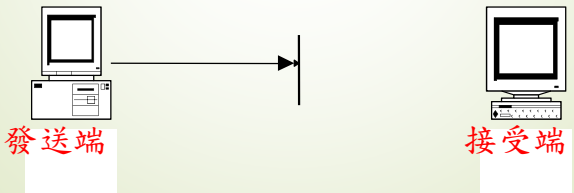
- 天然或人為
  - 天然災害
  - 管理人員的疏失
- 蓄意或無意
  - 企圖破解系統安全
  - 系統管理不良
- 主動或被動
  - 不會更改電腦系統資料
  - 電腦系統上資料會被篡改

網路攻擊

中途竊聽(Interception)



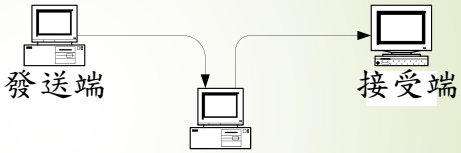
中斷、攔截(Interruption)



網路攻擊

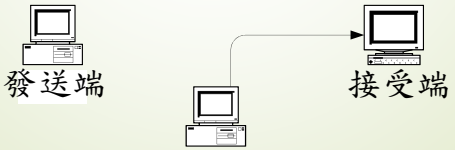
竄改(Modification)

不法之徒未經許可篡改資料。這類威脅有時比洩露機密資料造成更大損失。



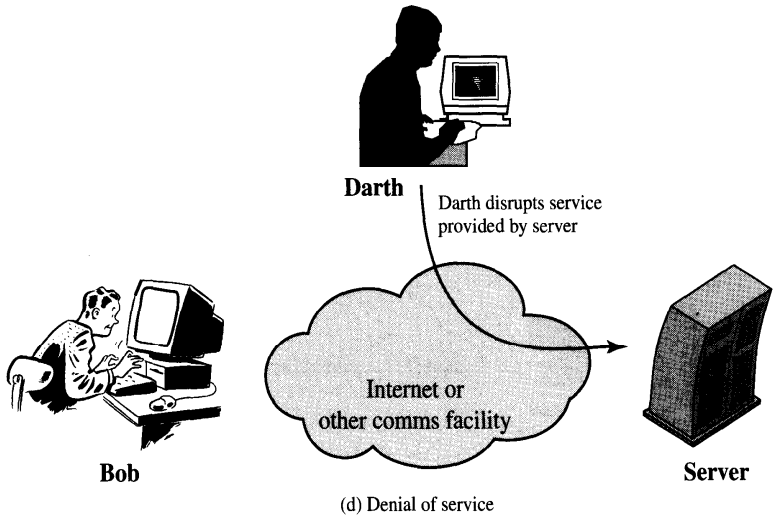
偽造(Fabrication)

與篡改威脅之不同點在於篡改之資料為已經存在之資料，偽造假資料則是無中生有。



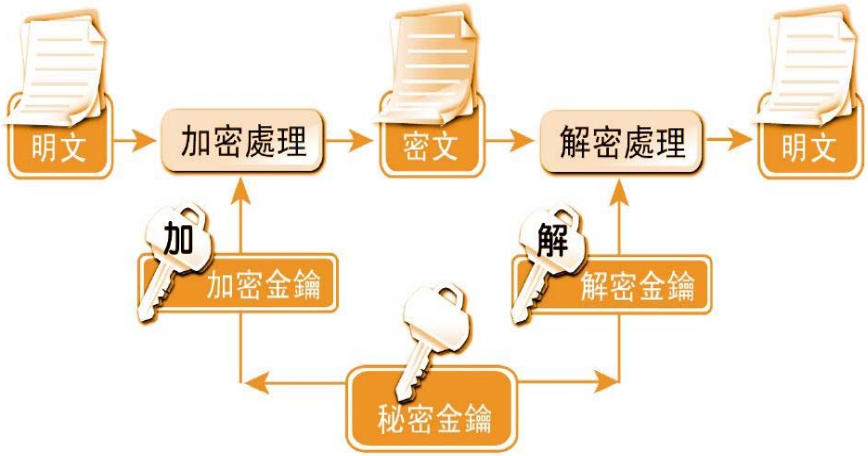
密碼學簡介

網路攻擊-阻斷服務 Denial of Service (DOS)



(d) Denial of service

加密系統架構



基本的加解密系統

密碼學的概念

- 加密 (Encryption)
  - 運用技術將要傳遞的訊息隱藏
- 中文範例
  - 清末大儒紀曉嵐贈送的對聯
    鳳遊禾蔭鳥飛去
    馬走蘆邊草不生
- 解密(謎)
  - 禾下加鳳去掉鳥字得禿字
    馬置蘆邊去掉草頭得驢字

清代紀曉嵐諷刺詩

「精神炯炯
老貌堂堂
烏巾白髯
龜鶴呈詳」

罵人 “精老烏龜”

中國古代密碼學

- 兵符
  - 是中國古代調兵或傳達命令所用的憑證，用銅、玉、木或石製成。形狀似虎，也稱作**虎符**。兵符製成兩半，一半留給君主，另一半交給下屬，須兩半符合後命令才能生效。
- 素書(密信)
  - **不成字**:是對文字進行拆解再重新加以排列組合，
  - **無形文**:是指以化學藥劑所書寫的文書，
  - **非紙簡**:是在書寫工具與資訊載體上動手腳。
- 〈六韜・龍韜・陰符〉 〈六韜・龍韜・陰書〉
- 攀書:明攀寫的書。
- 武則天時期 “青鵝” => 此26青字者，十二月。鵝字者，我自與也。”

密碼學在生活中的應用

- 密碼學與資料隱藏
  - 浮水印
    - 影像浮水印
    - 聲音浮水印
  - 條碼
    - 一維條碼
    - 二維條碼

一維條碼

- ·生活中隨處可見一維條碼
- ·取代KEY IN的動作
- ·條碼基本構造：
  1. 起始碼- 讀取器判別開始
  2. 資料碼- 照編碼方式
  3. 檢查碼- 確保資料正確
  4. 終止碼- 條碼結束

二維條碼(1/2)

Name	Figure	Manual
QR Code		Developed by TOYOTA subsidiary Denso Wave in 1994.
VS Code		Develop by Veritec in America.
SemaCode (Data Matrix)		Developed by a software company, Semacode based in Waterloo, Ontario, Canada.
Visual Code		Developed to enable HCI using camera phones.
Shot Code		Created by High Energy Magic of Cambridge University when developing TRIPCode.
Color Code		Developed by Colorzip and mainly used in Korea

1. 一維條碼用寬度記錄資訊
2. 二維條碼的長度與寬度都記錄資訊
3. Ex: QR code (Quick Response)

a. 三個角用來定位，較不受旋轉影響
b. 依照圖的大小最多能存數千個字

二維條碼(2/2)- QR -code

- 起源於日本, 為了追蹤汽車零件
- 在日本已相當普遍
- 2000年國際QR碼標準認可
- 應用
  - 文字、網頁、商品資訊、店家資訊
  - 電子票券、車票, ex: ibon上買的高鐵車票
  - 公車站牌上QR碼，掃一下可知
    班車時刻與路線並存於手機
  - Demo http://www.ipeen.com.tw/ 愛評網

中文WIKI網址的QR碼

資訊藏密 著作權 商標

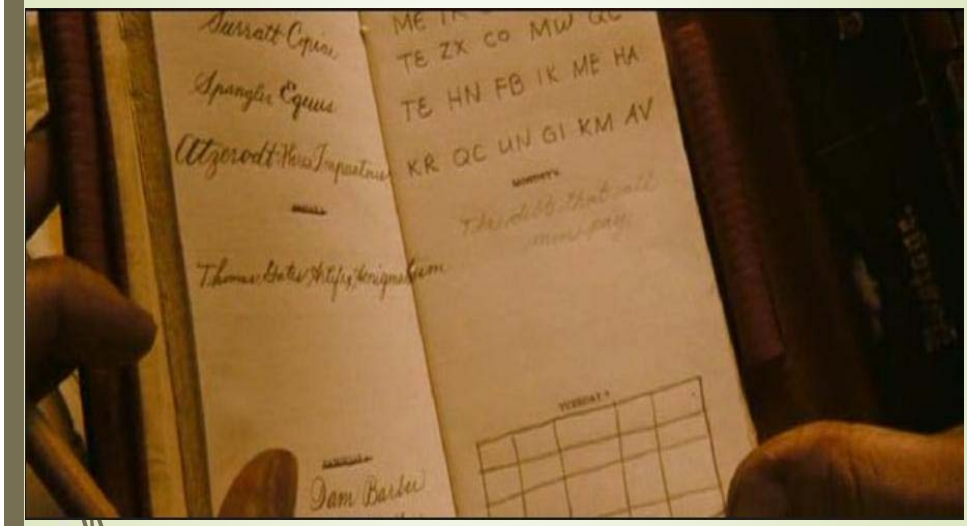
油畫影像

機場空照圖

浮水印

電影與密碼學

國家寶藏 http://mike0123783.pixnet.net/blog/post/32974942



Playfair 密碼

資料驗證、軟體驗證 (雜湊函數)

- 將任何長度的文件和資訊轉為特定碼數的代碼，稱為雜湊值，**明文一個小改變會影響一個範圍的雜湊值**
- 常見：MD2, MD4, MD5, SHA-0, SHA-1
- 應用：**確保資料完整性, ex：火漆**



軟體下載(含網路申報及二維條碼，Windows系統使用)

1. 個人綜合所得稅電子結算申報程式IRX14.05版 更新日期：102-05-23
   自動安裝版[15,700,806 位元組]建議使用。下載完成後直接執行即可進行安裝。SHA1驗證檔下載
   手動安裝版[11,781,290 位元組] 無法使用"自動安裝版"安裝者，請點選本版後選擇[執行]，選擇存放程式的路徑，並執行目錄下之setup.exe進行安裝。SHA1驗證檔下載
2. 執行業務暨其他所得者電子申報程式

凱薩密碼 Caesar Cipher-取代

- 記載於羅馬凱撒大帝所著《高盧戰記》Gallic Wars中及蘇東尼烏斯寫於西元二世紀的 《十二帝王傳》Lives of Caesars

0 1 2 3 4 5 6 7 8 9 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

範例 I LOVE YOU
=>
L ORYH BRX
Key =3

傳統密碼學

- 傳統密碼學的基本原理
  - 取代加密法 (Substitution Cipher)
    - A換成C, B換成D 等
  - 換位加密法 (Transposition Cipher)
    - 利用一個特定排列規則，將明文中的字元重新排列過，來產生另一個無規律的密文。

編碼法(Code Book)

隨機編碼本範例

明文	號碼
電腦	0711
資訊	1232
安全	2243
管理	3661
系	4538

『資訊管理系』：
1232 3661 4538

編碼本範例

明文	頁	位置
電腦	12	31
資訊	14	02
安全	18	24
管理	26	63
系	45	28
中興大學	65	84

『資訊管理系』：
14 02 26 63 45 28

墓碑銘文加密

■紐約州，Trinity市的墓碑

密文：

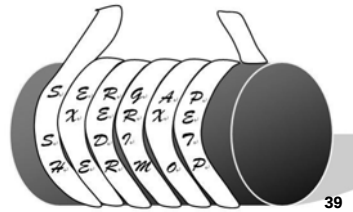
依照下列取代法則取代而成

A·	B·	C·	K:	L:	M:	T	U	V
D·	E·	F·	N:	O:	P:	W	X	Y
G·	H·	I·J·	Q:	R:	S:	Z		

密文：REMEMBERDEATE

古代的密文

西元前五世紀，古希臘採用斯巴達密碼棒(scytale)

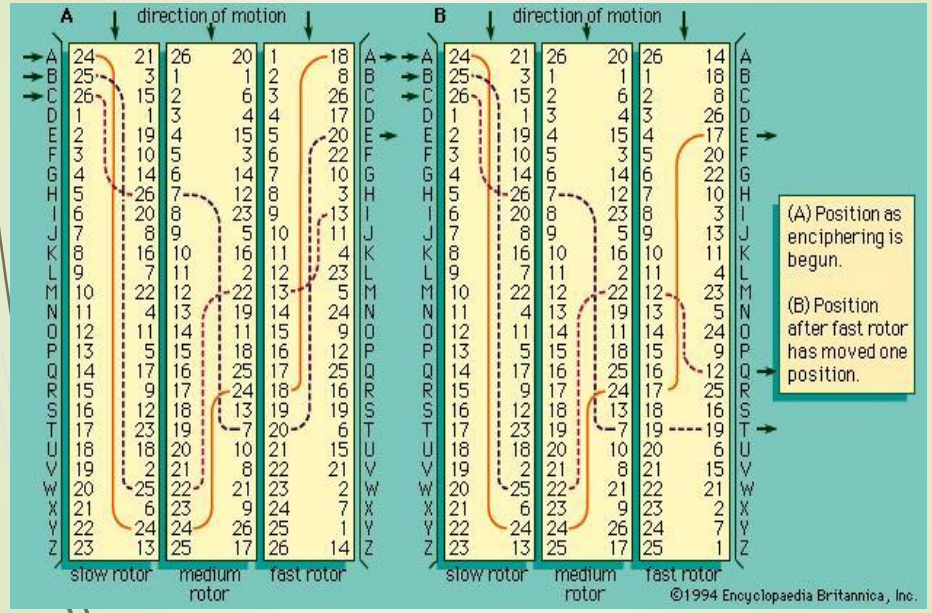


換位加密法

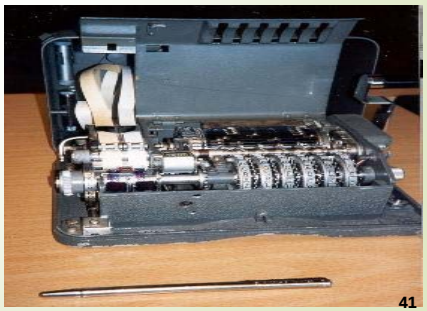
- 鑰匙排列法 (key =3412567)
  - 明文：I SIT BY MY WINDOW WAITING FOR YOU
  - 鑰匙排列：
  - 密文：IIIRTNTYSWAOIYWFBDIOYONUMWGE

鑰匙：	3	4	1	2	5	6	7
明文：	I	S	I	T	B	Y	M
	Y	W	I	N	D	O	W
	W	A	I	T	I	N	G
	F	O	R	Y	O	U	E

多重變換箱



Rotor Machine



密碼系統之安全性程度

- 無條件安全(Unconditionally Secure)

  非法使用者不管截獲多少個密文，用盡各種方法還是沒有足夠資訊可以導出明文機密資料。

- 計算安全(Computationally Secure)

  目前或未來預測之科技、以合理之資源設備下，要破解密碼系統需要一段相當長的時間（例如數百年）。

重要的加解密系統

- 資料加密標準 **Data Encryption Standard** (DES), 56 bits key, 1973
- **3-DES**, 112, 168 bits key
- 進階加密標準 **Advanced Encryption Standard** (AES), 2001, 192 bits key
- 公開金鑰加密**RSA**, 1978, MIT, 很大的質數 2^{200}~2^{1024}

安全性的假設

- 攻擊者可以利用各種方法收集明文與密文的關係
- 攻擊者可能知道加密的方法
- 所有加密解密的方法都須經過許多密碼學的許多專家的分析與攻擊，確保安全性
- 所有的安全性完全由**金鑰的長度**來決定，亦即，攻擊者需要花費多少時間或成本來破解金鑰。
  - **破解成本大於破解後所獲的利益**
  - **破解的時間超過所需要保密的時間**

key長度與破解難度之關係

Key Size (bits)	Key 的可能情形總數	10^6 次運算per sec.	10^{12} 次運算per sec.
32	$2^{32} = 4.3 \times 10^9$	2^{31} μs = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} μs = 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} μs = 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} μs = 5.9×10^{36} years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	2×10^{26} μs= 6.4×10^{12} years	6.4×10^6 years

網路安全傳輸機制

網路安全傳輸機制

- SSL(Secure Sockets Layer)
  - 此一網路資料安全協定是由Netscape首先發表。
  - SSL利用公開金鑰的加密技術(RSA)來做為用戶端與主機端在傳送機密資料時的加密通訊協定。
  - 已被大部份的Web Server及Browser廣泛使用。

2014/4/8
Heartbleed臭蟲已存在2年以上
Heartbleed臭蟲可讓他們無需權限資料就可以取得自己的x.509加密金鑰、用戶帳號、即時通訊、email及公司重要文件及通訊內容，而且完全不留任何痕跡。因此即使公司系統曾經遭到入侵，管理員可能也無從得知。

如何辨識SSL

1. 通訊協定是採用https://而非http://

2.出現上鎖的金鎖頭，表示支援SSL安全協定，按此可以開啟安全性報表並檢核憑證資訊

NCUE webmail SSL

網路信用卡認證

網路信用卡使用的問題

- 不肖廠商或程式設計師惡意記錄使用者卡號，安全號，姓名與個人資料偽造刷卡。
- 不肖程式人員架設釣魚網站竊取個資。
- 旅遊仲介人員離職前偽造業績盜刷。
- **半數使用Wi-Fi無線網路的零售店家沒有採取足夠的防護措施，使信用卡帳號等機密資料，可透過無線網路訊號輕易竊得。（美國 彭博資訊）**

什麼是〔Visa驗證〕與〔MasterCard驗證〕？

- 為兩種線上刷卡的安全付款機制。
- 商家結帳頁面看到的圖示，而且當您使用VISA或MasterCard信用卡時，將會和VISA/MasterCard組織以及您的發卡銀行連線。

VERIFIED by VISA
VISA驗證
MasterCard SecureCode

3D驗證密碼服務

- 以持卡人事先所設定的密碼來保護信用卡網路交易
- 只要持卡人完成註冊並設定好密碼之後，當每次至提供驗證服務的網路商店進行交易時，系統即會自動要求輸入密碼，並拒絕密碼錯誤的交易
- 降低卡片在網路上被偽冒的風險。

信用卡註冊

採用3D驗證的網站

網路金融卡

網路金融卡 –郵局網路ATM

郵局ATM 妨駭功能

- 動態鍵盤
  - 避免鍵盤側錄程式竊取密碼
- 圖形密碼
  - 避免程式惡意入侵與攻擊網站
- 抽拔卡機制
  - 確認轉帳繳費者確實擁有金融卡

郵局ATM 主畫面

郵局ATM 動態鍵盤

郵局ATM 交易明細表

- 建議列印或轉成pdf檔存檔

圖形密碼與動態鍵盤

自然人憑證

自然人憑證

- 自然人憑證就是網路身分證，也是推動電子化政府的基礎建設，其主要功能如下：
  - 確認身分
  - 保障資料傳輸安全
  - 確保交易之完整性與不可否認性
  - 保護隱私性

相關系統

- 內政部：
  - 戶政網路申辦服務系統、地政網路申辦服務系統、建築物公共安全檢查、個人有無限制出國查詢
- 交通部：
  - 電子公路監理網
- 經濟部：
  - 公司線上申辦系統、標準檢驗線上申辦管理系統、智慧財產權申請人/代理人登錄管理 系統

相關系統

- 財政部：
  - **網路申報繳稅系統**、稅務資料查詢、空運網際網路報關系統
- 行政院環境保護署：
  - 事業廢棄物管制系統
- 行政院國家科學委員會：
  - 研究人才個人網登錄、博士生/博士後個人網登錄
- 勞工保險局：
  - 勞保局網路申辦系統

憑證廢止

- **狀況：**
  - 本人懷疑或證實私密金鑰遭到破解
  - 憑證所記載之資訊重大改變，足以影響其信賴度（例如：用戶姓名變更)
  - 憑證永久不再需要使用
- **申辦方式：**
  - 用戶本人持身分證正本至戶政事務所自然人憑證櫃檯辦理（不限戶籍所在地均可辦理）

憑證停用

- **狀況：**
  - 憑證IC卡遺失或懷疑遭盜用
  - 自行認定必須暫時停用
- **申辦方式：下列二擇一**
  - 臨櫃辦理—用戶本人持身分證正本至戶政事務所自然人憑證櫃檯辦理。
  - 線上申辦：用戶可連線至自然人憑證專屬網站，選擇【憑證作業】/【憑證停用】功能，進行線上憑證停用程序。此作業須輸入「用戶代碼」以做為身份驗證之依據

網路安全實例與防範

近期的資安事件

微軟也遭駭！手法與Facebook及蘋果類似 都中了水坑式攻擊

2013年2月23日 13:50

【鉅亨網編譯呂燕智 綜合外

全球軟體龍頭微軟（Micros
意程式攻擊，情況與先前F
據顯示客戶資料受到影響；

微軟在官方部落格貼文指出
定暫時不公開宣布。

過去兩周，Facebook與蘋
意程式，所幸皆無資料遭竊

事實上，早從上個月開始包
續受到駭客攻擊，業內人士
東歐。

資安專家將最近這幾起事件稱為「水坑式攻擊(waterhole attacks)」，因駭客盯上的是有特定需求的受害族群而非特定公司，如同沙漠中的水坑一般，以此次風波來說對象就是程式開發人員。

免費Wi-Fi上網銀查看 轉眼戶頭被提領一空

2013-02-22 19:43 | 新聞速報 | 【中廣新聞／中廣新聞】

遇到無需輸入密碼即可免費使用的Wi-Fi未必是好事，有可能是遇上釣魚Wi-Fi，讓自己蒙受意想不到的損失。

大陸北京有一位男子報警說，他的銀行卡在深夜被分17次轉帳或取款，他唯一可能做的動作，就是睡前曾經用手機通過免費Wi-Fi登錄網上銀行查詢帳目而已。

網路安全專家指出，不法分子會設置沒有密碼的Wi-Fi吸引手機用戶使用。一旦連上釣魚Wi-Fi，手機用戶的操作記錄就會被複製，被相關軟體破解。15分鐘就可以盜走密碼。

專家說，用戶的賬號被盜分成兩種。如果網站加密性不高時，可能直接被不法分子破解。而安全係數高的如銀行等網站，駭客常會引導用戶到釣魚網站，進而獲取賬號和密碼。

因此專家建議，在同等條件下，從手機上的網銀官方手機客戶端登錄，會比用瀏覽器登錄網銀更爲安全。使用沒有密碼的免費Wi-Fi也要十分小心。

近年重大駭客攻擊事件

CYBERATTACKS TIMELINE

MAJOR COMPANIES/AGENCIES TARGETED RECENTLY

(Date of attacks only indicate when attacks were first discovered or publicised)

2010 Dec — Hacker group claiming attack — Mastercard.com, Paypal, Visa.com, PostFinance — Anonymous launches orchestrated attacks in support of Wikileaks founder Julian Assange

2011 Mar. (unidentified) — RSA — Hackers steal data related to RSA secure tokens

20 Apr or earlier — Sony Playstation Network — Lulzsec claimed to have stolen personal information from millions of users

22 Apr* — Fox Networks — Lulzsec stole personal information of 70,000 X Factor contestants, database and passwords from employees

May — Citigroup Inc. — Hackers take 200,000 customers' data

21 May — Lockheed Martin — Hacked but managed to stop attack before any critical data was stolen

30 May — PBS.org — Lulzsec defaced its website, posted a fake article and stole its database

1 Jun — Google — Email system hacked, attack suspected to originate from China

2 Jun 3 Jun — Sonybmg.nl, Sonybmg.be Nintendo.com Infragard-Atlanta (FBI)

10 Jun — Turkish government websites — Anonymous takes down several government sites in protest to Internet censorhip

11 Jun — International Monetary Fund — Hack suspected to originate from a "foreign government"

Spanish National Police — Anonymous hacks website in response to arrests of alleged group members

13 Jun — Bethesda Game Studio

U.S. Senate (www.senate.gov) — Lulzsec hacked and released internal data from its servers

15 Jun — Malaysian government websites — Hacked after an attack warning from Anonymous in response for censoring Wikileaks

Central Intelligence Agency — Lulzsec hacked the CIA's public website, www.cia.gov, making it temporarily inaccessible

駭客如何攻擊

- 最好是不必使用帳/密就進得了系統
- 最好使用者用的是**弱密碼12345**之類的或是使用在網路上就查得到的**系統預設密碼**
- 最好連上網路就可以順便**側錄帳號及密碼**
- 最好能變成最高權限等級的身份，不論是透過破解、非法或是合法取得的身份
- 最好程式開發商自己預留有**後門的萬能鑰匙**
- 找到後門後，就利用**Google Hacking**尋找全天下有相同漏洞的網站
- 駭客通常是不按牌理出牌，擁有惡搞一通的創意，而這思維模式違反正常程式開發者的思考邏輯

洩漏個資

單位	姓名	電話	帳號	E-Mail	密碼
總統府		02- -4159	L1207	mail.oop.gov.tw	
國家安全會議秘書處		02- -7302	T1202	@ms11.hinet.net	
研究發展考核委員會		02- -90636	F120	DSLDAP.gov.tw	
立法院		02- 5858	E1224	gov.tw	
國民大會		02 1312	F1219	ail.nasm.gov.tw	
選委會		02- 5217	A122	c.gov.tw	
行政院 海巡署		02- 9313	R121	cga.gov.tw	
經濟部 工業局		02- 1255	A104	moeaidb.gov.tw	
銓敘部 考選部		02- 9188	F2208	s.moex.gov.tw	
高雄 高等行政法院		07- 768	N120	udical.gov.tw	
交通部 臺灣鐵路管理局		02- 5226	J1016	tra.gov.tw	
福建省政府		08- 195	W100	ns1.gsn.gov.tw	
行政院 大陸委員會		02- -5589	K120	mac.gov.tw	
特殊帳號			gcaadm		
			admin		
族繁不及備載	.....	.....	.....	.....	.....

何謂網路釣魚

- **網路釣魚** (Phishing，唸法與 "fishing" 相同) 是一種網路詐騙手段，詐欺犯利用這種手段誘使您洩露個人資料。
- 網路釣魚最常見的目的就是騙取帳號及密碼。

釣魚攻擊

- 願者上鉤
  - 網路釣魚利用社交工程與技術性的詐騙手法，偽造**E-mail**或釣魚網站**(Phishing site)**，甚至採用綁架網址的方法，偷取使用者的**身分資料及金融帳號等機密資料**

釣魚網站

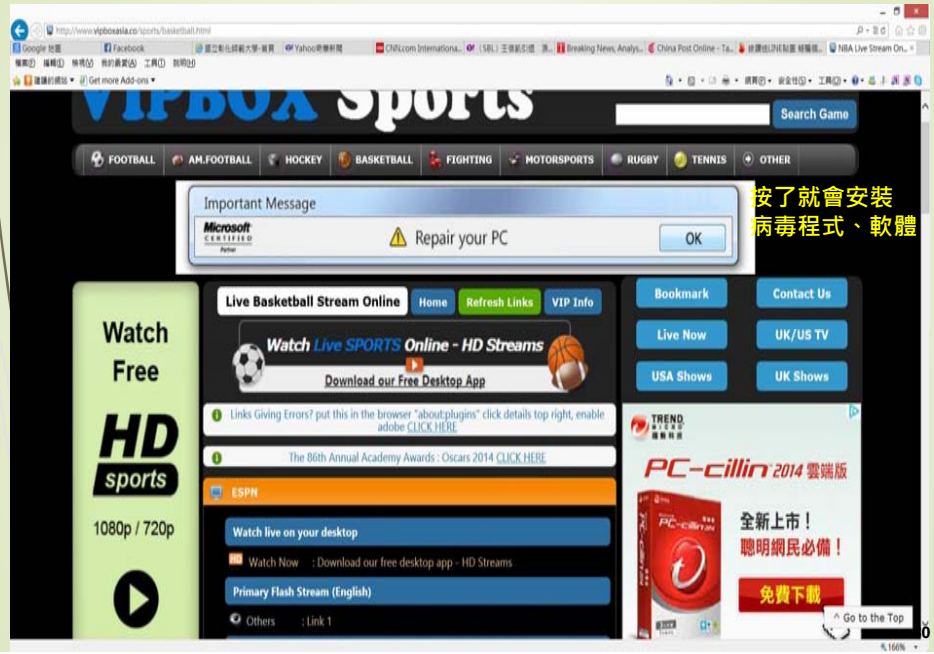
遠離網路釣魚犯罪陷阱與騙局

- 網路釣魚的防範訣竅：
  - ✓不回應任何來自不明單位於電子信件中要求提供個人隱私安全相關資訊，這些資訊包括使用者名稱、密碼、帳號。
  - ✓不點選來路不明的電子郵件中所載之網頁連結。
  - ✓不利用校園網路轉寄垃圾信函。
  - ✓點選網頁連結前請一定要仔細辨認。

網路釣魚新聞

- 新聞：臉書「露胸少女」？是駭客手法！
  - ✓駭客再度發動網路釣魚，這次目標鎖定Facebook、Twitter，以及Google+帳號密碼，全球資訊安全業者趨勢科技研究發現，近日在社群平台廣為流傳的「15歲少女在Facebook上露胸後自殺」影片實為暗藏惡意程式的有害影片，一旦點選影片，駭客將可以控制用戶個人帳號進行個資竊取等不法行為，並擴大感染範圍。
  - ✓運用聳動標題的連結進行網路釣魚已經是駭客必備技能之一。駭客在社群平台上散布「15歲少女在Facebook上露胸後自殺」的影片連結，點選該影片後將被**要求下載特定程式方能觀賞影片**，這個特定程式其實是木馬程式TROJ_FEBUSER.AA，這隻木馬程式會依據受害者使用的瀏覽器而偽裝成Chrome或是Mozilla Firefox的附加程式，讓使用者放心下載。

取自**2013.08.01聯合新聞網**



詐騙電子郵件案例分析

◆ 案例分析一：**信箱容量超過，請登入你的帳號、密碼？**

詐騙電子郵件案例分析

◆ 案例分析二：**希望有善心人士幫忙處理一筆鉅款？(國際詐騙)**

標題：Greetings Dearest Beloved,

內文：

I know that this letter may be a very big surprise to you, I came across your email contact from my personal search and I instructed the doctor here in this hospital to help me email you and i believe that you will be honest to fulfill my final wish before i will die.

I am Mrs Orgil Baatar, I am 66 years old ,From Mongolia, and I am suffering from a long time cancer of the breast. From all indication my condition is really deteriorating, and my doctors have courageously advised me that I may not live beyond the next one week; this is because the cancer has reached a critical stage.

I was married to late Dr Baatar Altangerel, gold & diamond exportation) in Burkina Faso, West Africa, where we live all our Lives for Thirty-two years before he died in the year2004. But is quite unfortunately, He died after a Cardiac Arteries Operation that lasted only for four days.

Since his death I decided not to re-marry, I deposited all the sum of$5.8million dollars with a Bank in Ouagadougou- Burkina Faso, where we spend our life together in Burkina Faso .

Presently, this money is still in their custody, and the management just wrote me as the Legitimate beneficiary to come forward to receive the money after keeping it for so long or rather issue a letter of authorization to somebody to receive it on my behalf since I cannot come over as a result of my illness, or they get it confiscated.

Presently, I'm with my laptop in a hospital where I have been undergoing treatment. I have since lost my ability to do anything myself and my doctors have told me that I have only 3 month to live.

Now that i am about to end the race like this, without any family members and no child. It is my last wish to see that this money is invested, but you will assure me that you will take 50% of the money and give 50% to the orphanages home in your country for my heart to rest.

I want your good humanitarian, to also use this money to fund churches, orphanages and widows around. I must let you know that this was a very hard decision, but I had to take a bold step towards this issue because I have no further option. I hope you will help see my last wishes come true.

As soon as I receive your reply I shall give you the contact of the Bank. I will also issue you a letter of authority which will prove that you are the new beneficiary of my funds, and the documents concerning the deposit. Please assure me that you will act accordingly as I stated herein. Hope to hear from you soonest. I am waiting your response.

Yours Sick Sister in Christ,

Mrs Orgil Baatar.

釣魚信件

寄件者: eBay <ebay@ebay.com> 收件者: deron@ms45.hinet.net <deron@ms45.hinet.net>
主旨: [X-Spam]Security alert

eBay sent this message to deron@ms45.hinet.net.
Your registered e-mail is included to show this message originated from eBay.

eBay confirmation form

Dear eBay user,

We would like to inform you that we have released a new version of eBay Confirmation form. This form is required to be completed by all eBay users.

Please follow these steps:
1.Open the form at http://cgi.ebay.com/ws/eBayISAPIdll?cfom=145682896443037672911987992574847391134140477151207.
2.Follow given instructions.

Thank you,
eBay

This eBay notice was sent to deron@ms45.hinet.net from eBay. Your account is registered on www.ebay.com. As outlined in our User Agreement, eBay will send you required notifications about format, change your notification preferences.

See our Privacy Policy and User Agreement if you have questions about eBay's communication policies.
Privacy Policy: http://pages.ebay.com/help/policies/privacy-policy.html
User Agreement: http://pages.ebay.com/help/policies/user-agreement.html

85

對可疑電子郵件應有警覺性

- ✓為何我會收到這封郵件？
  - ✓應確認寄件來源及寄件者
- ✓我是否應該收到這封郵件？
  - ✓應確認郵件主旨及郵件內容
- ✓我是否應該開啟這封郵件？
  - ✓是否與業務工作相關
  - ✓不開啟(點選)連結是否有影響
  - ✓審慎查證(寄件者)

86

電子郵件安全防制措施

- ✓電子郵件應「關閉預覽郵件」設定。
- ✓電子郵件應設定為「以純文字模式」開啟郵件。
- ✓不隨意開啟及轉寄與業務無關之電子郵件及網站。
- ✓不隨意點選或下載郵件內之連結與附件檔案。
- ✓如發現可疑信件應先與寄件者確認其真偽或通報資訊處查證。
- ✓不隨意開啟郵件(確認寄件人)。
- ✓不隨意開啟或下載附件。
- ✓善用密件收件人。
- ✓非必要不設定自動回覆。
- ✓不隨意留下郵件地址予他人。
- ✓注意陌生之寄件者。

87

網路釣魚的方法

- ◆砍站程式。
- ◆首頁植入惡意程式。
- ◆將DNS名稱更改其中一個英文字母。
  - ◆用數字1取代英文字母l。
  - ◆或用數字0取代英文字母O。
  - ◆xxx.com.tw或xxx.com。
- ◆發Email、廣告或簡訊。
- ◆Google搜尋排名。
- ◆向Google買關鍵字廣告。
- ◆偽站已存在很久。

88

如何防範釣魚網站

- 注意網址是否正確
- 自己輸入網址或使用書籤，而不要點選網站或E-Mail中的連結
- 注意網站是否與平常不同
- 網站是否要求過多的個人資料

辯識正確網址

- 比較看看那裡不一樣:

webmail.tku.edu.tw webmail.tku.eud.tw 淡江大學webmail
www.chinatrnst.com.tw www.chinatrust.com.tw 中國信託
www.ntx.gov.tw www.ntx.com.tw 財政部北區國稅局
TW.BID.YAHOO.COM TW.BlD.YAHO0.COM 雅虎拍賣
http://www.vvretch.cc/ http://www.wretch.cc/ 無名小站
http://www.pchome.com.tw http://www.pchorne.com.tw PCHome
service@1andbank.com.tw service@landbank.com.tw 土地銀行

辯識正確網址

- 比較看看那裡不一樣: (錯誤標紅色)

webmail.tku.edu.tw webmail.tku.eud.tw 淡江大學webmail
www.chinatrnst.com.tw www.chinatrust.com.tw 中國信託
www.ntx.gov.tw www.ntx.com.tw 財政部北區國稅局
TW.BID.YAHOO.COM TW.BlD.YAHO0.COM 雅虎拍賣
http://www.vvretch.cc/ http://www.wretch.cc/ 無名小站
http://www.pchome.com.tw http://www.pchorne.com.tw PCHome
service@1andbank.com.tw service@landbank.com.tw 土地銀行

Facebook 詐騙

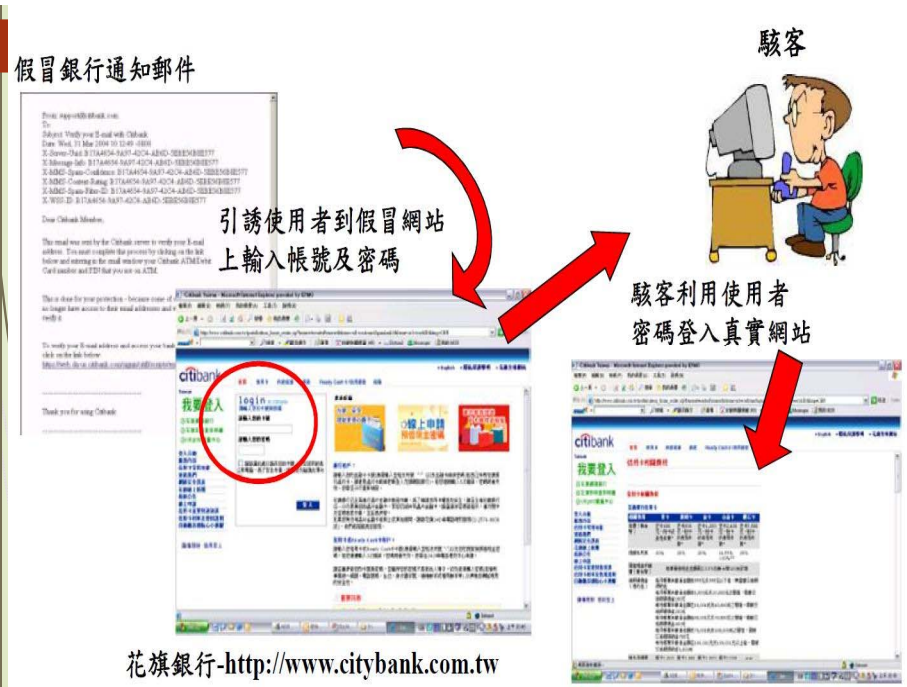
何謂社交工程

- 社交工程 (Social Engineering) 為利用人性的弱點進行詐騙，是一種非”全面”技術性的資訊安全攻擊方式，藉由人際關係的互動進行犯罪行為。
- 駭客通常由電話、Email或是假扮身份，問些看似無關緊要的問題等各種方法來進行社交工程。

利用Facebook進行詐騙

利用Facebook進行詐騙

- 詳細詐騙步驟
  - FB留言”方不方便用你手機幫我收一下簡訊？”
  - 利用因為朋友的關係請你告訴她手機號碼
  - 再到小額付費的消費網頁(EX:遊戲橘子)
  - 會發一封簡訊認證碼
  - 他再請你提供簡訊上的驗證碼
  - 該次消費即完成
  - 而你下個月帳單就會多1000元的消費紀錄
- 該手法已行之有年



《詐騙的購物社團特徵》

- 這類詐騙購物社團的共同特徵是：
  - 社員從數萬到數十萬人，而且大量新增中...
  - 所po出來的商品超低價，為了誘拐你上當...
  - 貨到付款，私訊要你留下姓名電話地址...（雖然一手交錢一手交貨，但其實他目的是要收集你的個資）
  - 通常管理員或po文者都是用美女大頭貼....（這是廢話，不然怎吸引你上當，美女照大多網路上隨意抓取的）

當你被加入類似上述購物社團請照以下步驟處理

- ▲檢舉與封鎖以下幾種人的帳號：
  - 該社團管理員與PO文的人...（這兩種人當然是主要的幕後黑手）
  - 你還可以檢視社團成員，就可看到誰在亂加人，通常都是被同一人大量加入...（這就是共犯）
  - 當然你可在動態上查看哪個好友把你加入社團的...（有可能他被盜帳號，你可以問清楚對方再處理）
- 通知帳號被盜的朋友，改密碼。

- 你在異性眼中的魅力有多少？
- 輸入你的身分證號碼後九位數，推斷明年運勢
- 賓拉登處決影片
- 未來1個月你會被什麼套牢？
- 你會成為百萬富翁嗎？
- 現在的你散發出來的愛情氣息是？
- 2011年的星座運勢如何？

資訊洩漏

1. 網路的資料從來沒有被真正刪除過
2. 交友資訊洩漏
3. 非自願性姓名洩漏
4. 住家、親人、工作地點、固定作息資訊洩漏
5. 臉部辨識技術
6. 地理位址辨識
7. 影像標記(Image tagging)

FB 隱私權設定

選擇安全強度高的密碼

- 選擇安全強度高的密碼，且不要和其他的網路服務共用同樣的帳號與密碼
- 重要帳戶的密碼不可重複
- 在密碼中混合使用字母、數字及符號
- 設定其他人難以猜到的密碼，避免簡單的字或組合，如 **password**、**letmein**、**abcd1234**
- 將密碼資訊保存在不易看到的隱密位置
- 時常更新密碼救援選項並確保其安全性

定期更新軟體

- 定期更新軟體
  - 瀏覽器、作業系統 **(Updated)**、防毒軟體
- 偶爾**google** 一下自己、家人看看是否有重要資訊被洩漏。
- 保持警覺、親友可能被駭。
- 絕對不點選不明來路的應用程式或遊戲要求。
- 經常變換密碼
  - 加減一個數字或文字
  - 至少每月變動
- 社交網路密碼、工作密碼、**e-mail**密碼、金融密碼區分

回報 Spam 或設定黑名單

手機使用安全與病毒

Facebook打卡好不好？！

◆ 新聞：臉書打卡露餡　債主闖咖啡廳強押人。

被害人因為生日到咖啡廳打卡，從臉書上暴露自己的行蹤。

◆ 新聞：打完卡外出買早餐 車禍不算職災。

勞保局說，打卡後買早餐，不能算是公務，但如果在打卡前出意外，都能算是職業災害。

◆ 新聞：循臉書打卡 警追回失蹤少女。

警方訪查少女好友，從少女友人臉書打卡紀錄找到離家少女。

打卡 = 告訴大家你人在那裡

Android安裝APP注意事項

- 安裝來源
  - 該選項不要勾選

  (當該選項為勾選時，將有很大的風險下載惡意程式。)
  - 儘可能確保軟體來自於合法的官方軟體商店(如App Store、Google Play)

Android安裝APP注意事項

- 注意星級與評等數
  - Google store 有提供星級與評等來了解APP的優劣狀況，但並非4星或5星就是好的APP，應該配合總評數及使用者評論，更進一步了解該APP的安全及可用度。

Android安裝APP注意事項

- 查看APP存取權限
  - 在下載APP時，頁面會出現該APP所需要的權限，安裝時請針對這部分進行留意，不要貿然安裝。

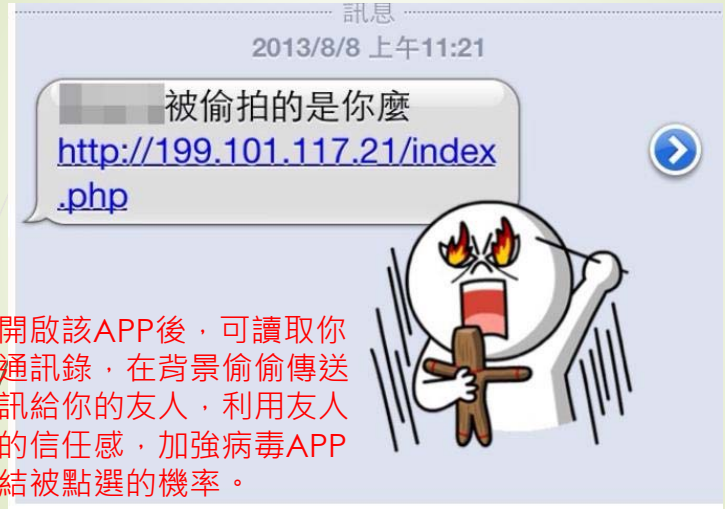
留意 APP 病毒軟體

- 假 Mac OS安裝程式
  - 透過手機帳戶向使用者收錢
- 追蹤電話與手機位置的Android間諜軟體下載次數高達10萬次
- 假壞蛋豬/搗蛋豬（Bad Piggies）遊戲,一下載即亂發簡訊,受駭者買單
- <惡意Android app>假太陽能充電應用程式,用假正面評價騙取下載,附贈偷資料病毒
- Google Play上出現假的Adobe Flash Player，是內含一堆廣告的惡意程式，請勿下載安裝！

詐騙進階版

- 手機病毒大揭密，那些您不知道的事：小心病毒使帳單爆增！
  - 我們可以歸納出整個惡意的流程：
    - 駭客依據收集到的電話清單，發送吸引你去點擊的簡訊內容！
    - 收到駭客所發送的簡訊後，點擊簡訊內的URL，下載了一個惡意的APK！
    - 利用社交工程以及人性的恐懼，譬如收到好友傳來的訊息：「你的照片被偷拍了，快點選 http://goo.gl/oxoxoxo下載」、或是好奇心：「這是我最新的寫真照，來看看吧 http://goo.gl/xoxoxoxox 」。
    - 駭客利用你的電話號碼來謀取小額付費的利益、竊取你的簡訊及幫他散播病毒！

手機簡訊詐騙



當開啟該APP後，可讀取你的通訊錄，在背景偷偷傳送簡訊給你的友人，利用友人間的信任感，加強病毒APP連結被點選的機率。

小額付款機制的風險

- 電信商有一種小額付款的機制，當購買後，電信商會傳回認證碼要求使用者確認，可參考165說明 http://165.gov.tw/fraud.aspx?id=21 。
- **Android 的開放技術，允許第三方程式：**
  - **自動送出簡訊、自動讀取簡訊、自動刪除簡訊。**
  - 因此這個病毒木馬APP，可以做到自動消費、自動回傳認證碼，順便再把相關的簡訊刪除掉，讓使用者在不知情的狀況下，只有隔月收到帳單才知道已經當了冤大頭。

代收驗證碼 用LINE詐87人

歹徒冒友索個資「關閉小額付費」

2013年11月25日 讚 2,112 +1 3

歹徒利用LINE進行小額付款詐騙，近半個月已

【林志青\台北報導】好友求助簡訊務必查證！手機通訊軟體詐騙案越來越多，警方發現歹徒利用即時通訊軟體LINE，佯裝被害人好友，要求代收簡訊，藉機騙身分證號碼及電信小額付款密碼，刑事局統計本月一至十八日，全台就有八十七人上當，每人被騙金額從一千至六千元不等。

根據警政署統計，八月開始出現LINE詐騙手法，三個月來有六百七十四人被騙了一百七十七萬元。

桃園吳姓男子接到手機簡訊:「老同學來看我現在的照片，能想起來我是誰嗎」，吳男好奇點選連結，並依網頁指示下載手機應用程式，雖然有看到一些照片，但他根本不認識，不到一小時即接獲電信公司傳來簡訊，通知付費六千元，才知道上當了。

LINE 詐騙

QR碼藏「木馬」　攔截簡訊、盜空帳戶

- 用手機掃描QR CODE來登錄網頁，已經成為許多人習慣的方式，不過在大陸，最近卻發生有不法份子，用各種不同的方式，引誘被害人掃描隱藏有木馬程式的QR CODE，進而盜取被害人個資，最終把被害人的存在第三方支付網站，跟銀行帳戶裡的錢，都盜領一空。

大陸這位余小姐，在網路商城賣東西，已經很有經驗，但不久前，一則客戶留言，卻讓她吃了大虧。電信詐騙被害人余小姐：「他就說我要買的東西呀，像那個照片啊實物啊尺寸啊，像那個照片啊實物啊尺寸啊，都在二維碼(QR CODE)裡面，叫我用手機掃一下看，就能知道啦。」

下載了QR CODE，卻點不開網頁，對方又請余小姐乾脆給他手機號碼，方便直接聯絡，沒想到，電話號碼剛給出去，一個小時內，余小姐從在銀行帳戶跟第三方支付網站裡的2萬多元台幣全被轉走。大陸網路工程師：「讓你點安裝，實際上就是把木馬給安上了，短信(簡訊)竊取的木馬，你的短信就被他監控了。」

聽懂了嗎？不法份子引誘被害人掃描QRCODE，在她手機植入木馬程式，就可以上網更改她的支付密碼，依照現行的網路安全措施，網路業者，會把驗證碼，用手機簡訊發給被害人，歹徒等的就是這個，為了成功引誘被害人下載木馬程式，歹徒甚至連手機基地台，都能偽裝。

大陸網路工程師：「你的手機走進我這個，(偽裝基地台)信號範圍之內，就會被這個偽基站吸進來，(來電顯示偽裝成)你比較熟悉的，官方的號碼你會比較信任，很容易就中招(被騙)了。」

雖然想要更改帳戶密碼，還需要被害人身分證字號等資料，但在如今，這些個人資料根本不算秘密，大陸網路業者坦言，手機網路支付並不安全，在新技術研發前，用戶只能自己小心，陌生人給的QRCODE別亂掃描。

你不能相信 LINE 的 13 句話

- 「OOO這是你那晚沒來的照片，我被整慘了...」
- 「OOO我在墾丁拍的照片，你覺得哪張最好看。」
- 「OOO這是上次同學聚會的照片，大家都有來」，
- 「OOO朋友家狗狗參加人氣比拼，幫忙讚一下」
- 「OOO這是上次聚會的照片，你好好笑」
- 「是OOO麼？老同學來看我現在的照片能想起來我是誰嗎..」
- 「OOO看著這些照片，好懷念以前的日子！」
- 「OOO被偷拍的是你嗎?
- 「OOO看看你以前的模樣」
- 「OOO那些年你年輕的模樣」
- 「OOO我們中秋烤肉的照片,好多人喔」
- 「OOO朋友參加攝影比賽幫忙投票」
- 假冒出差同事發送line,代收包裹

七步驟防止手機病毒跟著走

1. 接收藍芽傳送檔案要特別謹慎，以免收到病毒檔案
2. 不慎中毒暫時關閉手機上的藍芽接收功能，以免繼續搜尋感染目標
3. 收到來路不明的簡訊，不要打開直接刪除
4. 對於來路不明的手機程式不要任意安裝
5. 下載手機鈴聲、手機遊戲，請至合法官方網站
6. 若不慎中毒請立即刪除病毒應用程式，並重新安裝受感染的應用程式
7. 安裝手機病毒軟體

簡報完畢，敬請指教。