symantec™

Confidence in a connected world.

資訊安全講座
網路安全威脅及入侵手法解析

藍允澤 / Danny Lan

上奇科技

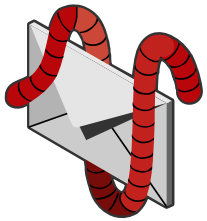
弱點在哪裡?

- 問題：如果您有一百萬元美金，您會如何破解最高等級的安全系統?
- 找駭客幫忙? 還是?

從內部下手可能是最快的!!

我們每天所面臨的威脅

Whale Phishing



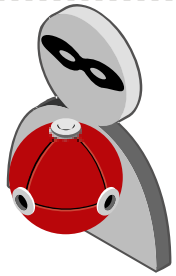
Security Risk

Browser help object

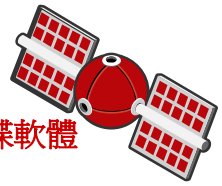
Code Red

0-day attacks

malicious macro program



Apply delta file to hub



間諜軟體

segmented definitions

郵件蠕蟲

application filtering from firewall

Botherder or Botmaster

iFrame attack

protecting identified vulnerabilities in software code.

patch strategy

Attacking the vulnerabilities of a computer

犯罪軟體

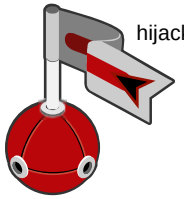
installation and code execution done without end-user consent or knowledge

Unauthorized act of bypassing the security mechanisms

Zero Day Threat

stealing and assuming another person's identity

Generic exploit blocking



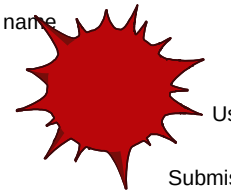
hijacking a Web site's domain name

Marco Virus

WebAuth and WCID

Drive-by-Download

Malicious Code



Polymorphic Virus

Keystroke logger

User mode rootkits intercept system calls

Stealth Virus

Snoopware

Submission of samples for collection and analysis

Travckware

傀儡網路

病毒

垃圾郵件

Minimize the impact of vulnerabilities

Blacklist

Security Alert

heuristic problem-solving techniques

AntiVirus

Phishing sites use "zombie" networks of hijacked computers

Firewall

Sending emails with a virus attached

Melissa

On-demand file system scanning

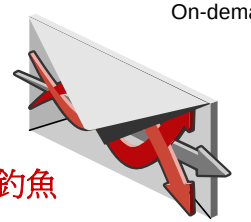
comprehensive security solution that includes a layered approach

distinguish behaviors of legitimate applications from malicious ones

Browser plug-in vulnerability

Spyware

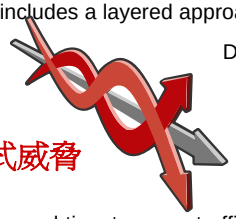
DeepSight



Adware

Trojan

Hoax



混合式威脅

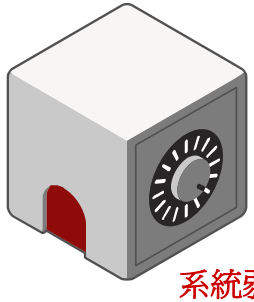
網路釣魚

Global Intelligence Network

real-time two-way traffic analysis

Behavioral Malware Detection

signature-based protection



access over the Internet from another compute

propagating by multiple methods, attacking from multiple points, spreading rapidly

Variants

系統弱點

Device protection

攻擊者爲了達到目的，利用各種手法攻擊使用者

“偽裝”

好玩的遊戲

有趣的內容

“誘騙”

好康的資訊

精采的圖片

最終目的都是希望使用者能開啓檔案

symantec™

Confidence in a connected world.

常見的網路安全威脅

上奇科技

惡意程式碼

- 電腦病毒的特徵
  - 會不斷「自我繁殖」及「感染」
  - 會有「潛伏期」
  - 會直接或間接的影響電腦系統運作，損壞軟硬體或資訊
- 電腦病毒的存在方式
  - 隱藏在開機磁區中
  - 寄存在可被執行的檔案之中
  - 隱藏在正常的檔案之中
    - 圖片、MP3、影片、壓縮檔、文件 …
  - 偽裝成系統檔案

隱藏的安全風險

- 什麼是安全風險
  - 通常對系統沒有立即的威脅
  - 沒有自我複製、感染及攻擊能力
  - 通常是使用者在不知情的情況下被下載安裝
  - 可能是好用的小工具但也可被利用爲攻擊的工具
- 安全風險可能造成的影響
  - 敏感性資料的流出
    - 帳號、密碼、個人身分資料、信用卡資料…
  - 設定遭到更改，無法恢復原本的設定
    - 網頁綁架
  - 應用程式出現不曾安裝過的額外元件
  - 電腦及網路受到影響
    - 電腦反應遲緩或網路效能降低
    - 系統不穩定或發生異常現象
  - 不斷從網路上下載惡意程式

系統入侵

- 系統或程式弱點
  - Windows OS、Internet Explorer、Office…
  - WWW、FTP、SMTP…
  - MS SQL、MySQL…
- 密碼猜測
  - 常用密碼字典檔
  - 暴力破解法
- 其他手法
  - SQL Injection

網路釣魚 (Phishing)

- 釣魚攻擊的操作手法和數量已超越一般電腦病毒和木馬程式，成爲網路安全的最大威脅。
- 利用僞造電子郵件或網站作爲誘餌，且利用知名公司所建立的信賴感，提高詐騙的成功機率，讓受害者洩漏個人資料
- 主要在於騙取受害著的身分證字號、銀行帳號、密碼、信用卡號碼等機密資料
- 常見的網路釣魚方式
  - 詐騙網址
  - 電子郵件表單
  - 彈出式的視窗
  - 僞造 IE 網址列
  - 僞造知名網站

symantec™

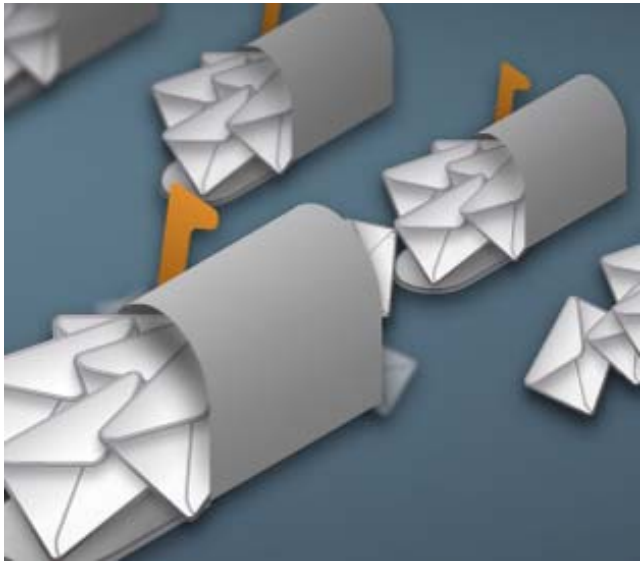
Confidence in a connected world.

常見的威脅入侵管道

上奇科技

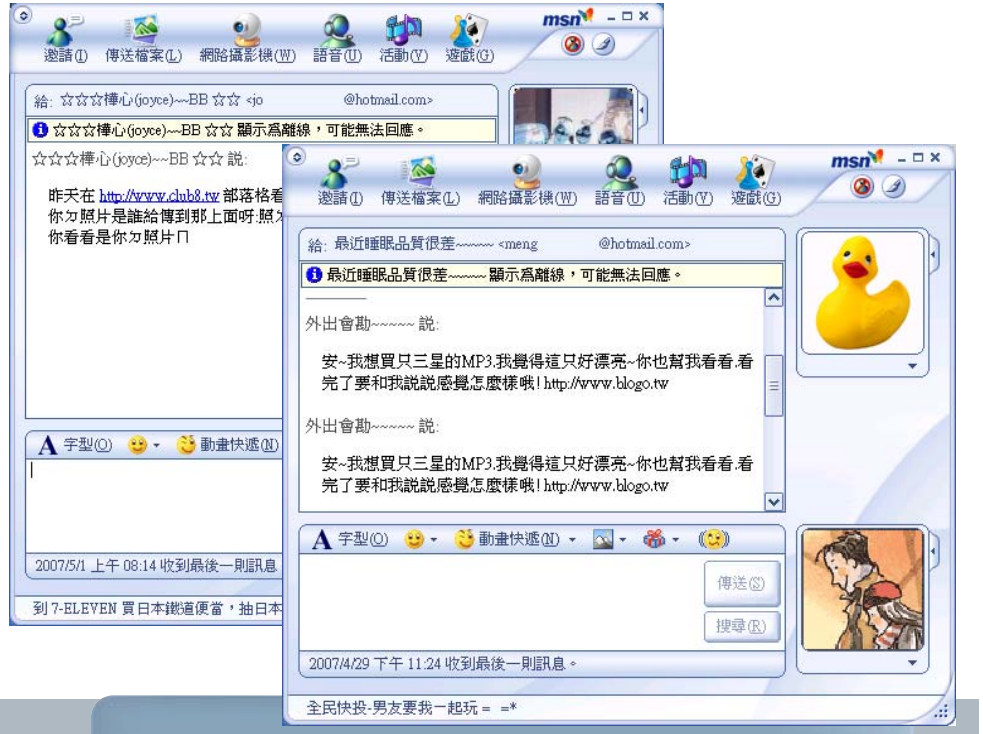
常見的威脅入侵管道：電子郵件

- 電子郵件已經成爲不可或缺的通訊工具
- 接收的電子郵件可能含有惡意內容
  - 60% 以上的電子郵件是垃圾郵件
  - 80% 的病毒經由電子郵件閘道進入組織
- 惡意郵件可從以下管道入侵
  - 透過技術手段大量從互聯網上隨機截獲郵件地址
    - 部落格、含有個人資訊的網頁、BBS …
  - 透過網上註冊認證、發展會員等方式收集電子信箱地址
    - 論壇、交友網站、購物網站…
  - 利用技術直接攻擊郵件主機
    - 字典攻擊
    - 郵件主機的弱點



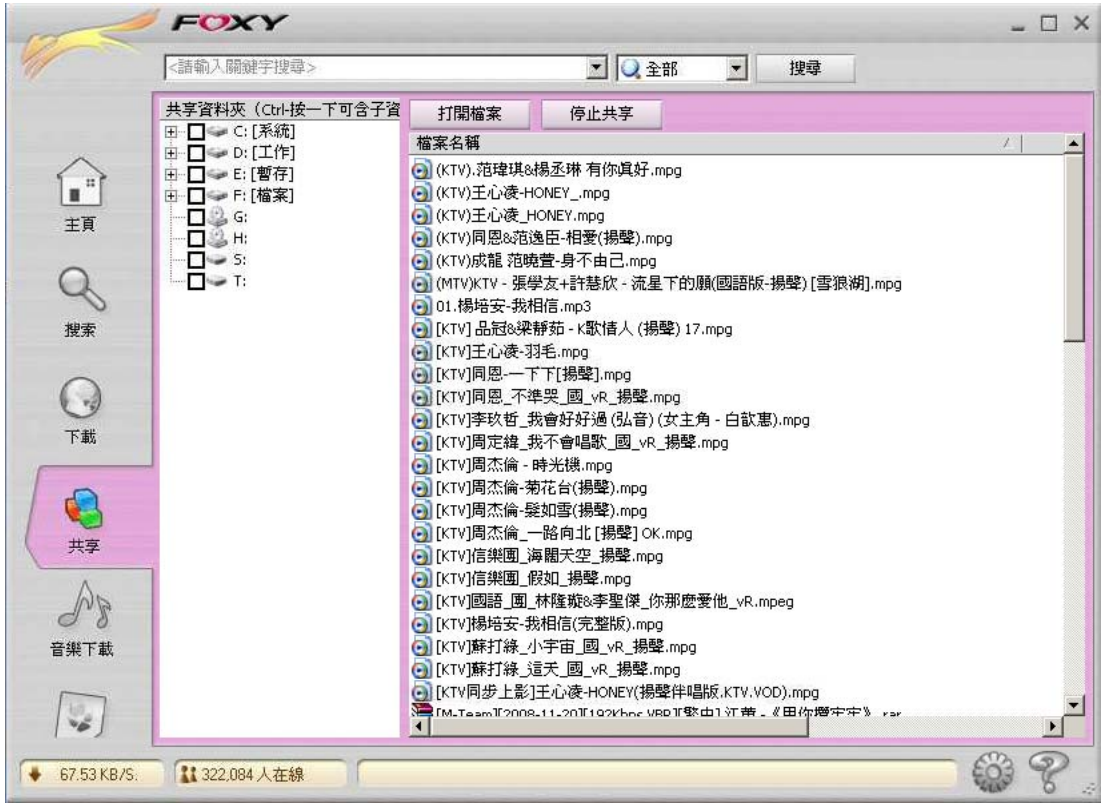
常見的威脅入侵管道：即時通訊軟體

- 什麼是即時通訊軟體?
  - 即時通訊（Instant messaging，簡稱IM）是一種即時通訊系統，允許兩人或多人使用網路即時的傳遞文字訊息、檔案、語音與視訊交流。
  - 即時通訊軟體擁有可多工作業、非同步性、長短溝通、媒介轉換迅速、互動性以及不受時空限制等特性，廣受使用者喜愛，甚至許多商業活動也會利用即時通訊軟體進行，以增進溝通效率。
- 使用即時通訊軟體的風險
  - 無法及時分辨檔案及訊息的可靠性
  - 訊息散播快速
- 常見的即時通訊軟體
  - MSN Messenger
  - Yahoo! Messenger
  - Skype
  - QQ



常見的威脅入侵管道：檔案共享軟體

- 什麼是 P2P 檔案共享軟體?
  - P2P 是 Peer-to-Peer 的簡寫，意思就是參與其中的所有角色都是平等互惠的，由所有的使用者直接互相分享。
- 使用檔案共享軟體的風險
  - 會共享預設資料夾中的檔案
  - 會無限制的使用頻寬
  - 無法過濾下載的檔案來源
- 常見的 P2P 檔案共享軟體
  - BitTorrent
  - eMule
  - FOXY



常見的威脅入侵管道：外接式儲存裝置

- 什麼是隨身碟病毒?
  - 隨身碟病毒又稱 Autorun 病毒，是一種透過 autorun.inf 檔案以及作業系統的特性，經由 USB 隨身碟或外接式硬碟傳遞的惡意程式
- 隨身碟病毒的興起
  - 隨著 USB 隨身碟、外接式硬碟、儲存卡等移動式儲存裝置的普及，移動式儲存裝置已逐漸取代傳統的磁碟片，成爲最主要的檔案傳遞媒介
  - 自 Microsoft 推出 Windows XP 後，開始利用 autorun.inf 讓使用者可以在使用外接式裝置時，自動執行指定的指令以方便使用者
- 已知的隨身碟病毒
  - W32.Gammima.AG (KAVO)
  - W32.Downadup.B (Conficker、Kido)
  - …

symantec™

Confidence in a connected world.

惡意威脅入侵手法解析

上奇科技

木馬屠城記

致命的特洛伊木馬(Trojan)

- 特洛伊木馬程式就像神話中所述的一樣，看起來像是一件禮物，但結果卻是一些突擊特洛伊城的希臘士兵
- 一種會在被感染的電腦中背景執行的小程式，看似有用，但實際上卻會造成損害
  - 安全性更新程式、掃毒軟體、廣告軟體移除工具
  - 有趣的小遊戲
- 通常都會以一些特殊管道進入使用者的電腦系統中，然後伺機執行其惡意行爲
  - 格式化磁碟
  - 竊取、刪除檔案
  - 竊取密碼
- 會竊取電腦中的隱私極重要資料，更是駭客常用的程式工具
- 引誘使用者開啓程式，藉而將特洛伊木馬程式植入系統
- 一些免費或共享軟體也可能包含特洛伊木馬程式

惡意威脅的入侵手法解析

- 駭客利用工具將惡意程式偽裝
  - 照片、小遊戲、掃毒軟體、工具…
- 透過網路散播含有惡意程式的檔案
  - 放在網站上或透過P2P軟體供人下載
  - 傳遞給 Mail 或即時通訊軟體上的好友名單
- 誘騙使用者接收並開啓惡意程式
  - 告訴使用者是好用的工具或好玩的遊戲
  - 透過文字說明誘騙使用者點選網址
  - 帥哥美女照
- 取得敏感性資料
  - 帳號、密碼、 個人資料…
- 儘可能隱藏自己的行蹤
  - 變更檔案屬性、檔名或變更系統設定
  - 從網路下載新版本更新以逃避防毒軟體的掃描
- 利用各種手法尋找下一個攻擊目標

實機展示

- 展示一：駭客如何將執行檔偽裝在圖片或音樂檔之中

- 展示二：駭客如何取得使用者帳號密碼

如何降低中毒風險?

- 不開啓來路不明的電子郵件
- 不瀏覽風險較高的網站
- 再三確認網址，避免使用超連結
  - 超連結的真面目
    - <A HREF="http://www.symantec.com.tw">http://www.symantec.com.tw</A>
  - 駭客喜歡玩的文字遊戲
    - www.citibank.com.tw 與 www.citybank.com.tw
    - www.paypal.com 、 www.paypaI.com 與 www.paypa1.com
- 絕不下載或開啓來路不明的檔案
  - 圖片、影片、MP3
  - 壓縮檔
  - Word、Excel
- 不使用來路不明的軟體
  - 有趣的小遊戲
  - 免費軟體或共享軟體
  - 盜版軟體、好用的工具

symantec™

Confidence in a connected world.

資訊安全不是只有防毒而已

上奇科技

隱而不見的危機

- 古有云：「內賊難防」
  - 『人性因素』才是安全措施中最弱的一環
  - 最好的防護技術也無法完全防止使用不當所帶來的危害
  - 任何的粗心或不在意都有可能造成資安的損失
- 只要一通電話就可以造成的威脅
  - 個人資料外洩
  - 帳號密碼被盜用
  - 機密資料被竊取
  - 植入惡意程式
  - 身分冒用
  - …

社交工程術 (Social Engineering)

- 『跟你裝熟，以達到特定的目的』
  - 利用人性弱點或人際互動上的技巧進行巧妙的騙術，以影響力與說服力來欺騙他人或令對方相信其假冒的身分，進而獲取資料的行爲
  - 社交工程駭客得以利用他人，不管有無動用到科技、電腦或程式，都可以獲取帳號、密碼、信用卡號碼、身分證號碼、姓名、地址或其他可確認身分或機密資料
- 社交工程術是最難防禦的攻擊手法

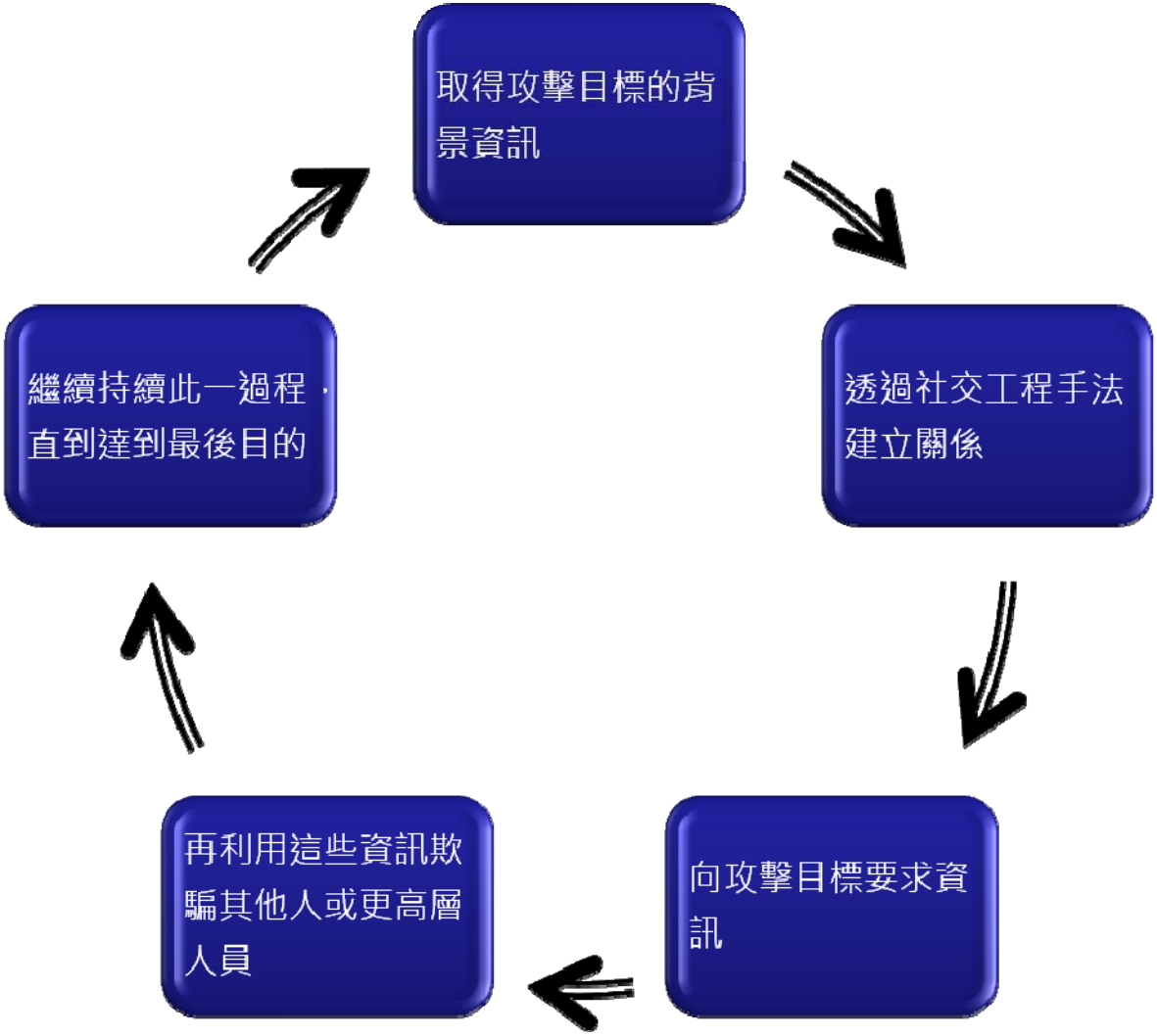
沒關係?? 很有關係!!

- 資訊中潛藏的價值
  - 很多內部表面上無傷大雅的資訊，卻都備受社交工程駭客的青睞
  - 駭客可以將表面上沒有價值的資訊加以利用，以取得對自己更有價值的資訊
- 任何資源都可以提供足夠的資訊
  - 公司名稱、系統管理人員、聯絡人電話或E-Mail 信箱、地址等基本資訊
  - 利用網站、報紙、搜尋引擎、信件、廢紙

網路上什麼都有

- 您知道您的資料已經上網了嗎?
- 網路上可以找得到的東西比您想像中還要多

社交工程手法解析


取得攻擊目標的背景資訊
透過社交工程手法建立關係
向攻擊目標要求資訊
再利用這些資訊欺騙其他人或更高層人員
繼續持續此一過程，直到達到最後目的

常見的社交工程手法

- 假冒同事
- 假冒廠商、合作夥伴、或是執法單位的員工
- 假冒具有權威的人
- 假冒新進員工，需要幫忙
- 請求總機幫忙接傳真，然後再要求轉傳
- 請求將檔案傳至公司內部的地方
- 謊稱是公司外地員工，要求設立可以在當地存取的電子郵件
- 使用內行人術語和行話來取得信任
- 假冒廠商打電話來提供系統修補程式或更新程式
- 告訴對方如果發生問題可以找他，然後製造問題，讓對方打電話來求援
- …

常見的社交工程目標

- 不了解資訊重要性的人
  - 總機人員、工讀生、行政助理、警衛…
- 有特權的人
  - 服務中心或技術支援、系統管理員、電腦操作員、電話系統管理員
- 系統製造商或廠商
  - 電腦軟硬體製造商、語音信箱系統廠商、網路或系統維護廠商
- 特定部門
  - 會計、人力資源

容易受社交工程攻擊的原因

- 員工人數眾多
- 辦公地點眾多
- 員工在語音信箱中告知去處
- 透露電話分機資訊
- 缺乏安全訓練
- 缺乏資料分級體系
- 缺乏事件通報或反應計劃

真實案例解析 (2006-02-11)

總機：「XXX科技您好」

駭客：「妳好，請問 Trista 在嗎？」

總機：「她現在不在座位上，需要我幫您留言嗎？」

駭客：「沒關係，我只是要寄個東西給 Trista，可是我不太確定妳們公司的地址，妳能夠告訴我妳們公司的地址嗎？」

總機：「沒問題，我們的地址是台北市長安東路一段xx號xx樓之3。」

駭客：「謝謝，請問我只要寫 Trista 收，她就會收到了嗎？」

總機：「沒錯，不然你也可以寫給許xx小姐收。」

駭客：「請問她的分機號碼是？」

總機：「她的分機號碼是XXXX」

駭客：「這樣我知道了，謝謝妳！」

總機：「不客氣」

我們可以做什麼?

- 多問一句
  - 保持懷疑，儘可能確認對方身分及目的
- 在無法確認對方身分前，不要任意告知任何內部資訊
- 保護好自己的個人資訊
  - 避免參加來路不明的有獎調查等活動
  - 不要把郵件地址在網路上隨意登記或告訴不信任的人
  - 根據不同的目的使用多個電子郵件地址
  - 不要在網路上公開個人資訊
  - 不要將個人資料任意丟棄

Thank you!

dannylan@pixnet.net
http://security.magicworks.net

上奇科技