社交工程

計算機與通訊中心
網路系統組 陳怡碩
E-mail：yschen@cc.nthu.edu.tw
分機：31234

Outline

- 社交工程介紹
- 教育部惡意電子郵件社交工程演練信件標題
- 社交工程的防護
- 網際網路服務介紹

社交工程

- 社交工程的定義
  - 利用人性弱點或利用人際之信任關係來進行詐騙，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。
  - 社交工程陷阱這個名詞來自駭客出身的資安顧問 – Kevin Mitnick，它是種引誘人們做出本意不想的行為，或是給出機密資料。欺騙的藝術(The Art of Deception)的作者（Kevin Mitnick），更進一步的解釋到人類的天性就是很希望能幫助別人，因此也相當容易被欺騙。
  - 網路世界的數位安全(Secrets & Lies: Digital Security in a Networked World)的作者Bruce Schneier曾提到所謂社交工程，全都是由人性方面，也就是利用所謂的「信任」來進行。
  - 以人為本、騙術為主
  - 技術門檻低
  - 貪心、好奇
  - 缺乏警覺性：有那麼嚴重嗎？

社交工程詐騙成功的結果

- 垃圾信的發信主機
- 機密資料外洩
- 攻擊他人主機的跳板
- 非法資料的存放主機
- …

社交工程攻擊的方式

- 早期社交工程是藉由電話或假扮身份問些看似無關緊要的問題等各種方法來獲取所需資訊。
- 透過電子郵件進行攻擊之常見手法
  - 假冒寄件者
  - 使用與業務相關或令人感興趣的郵件內容
  - 含有惡意程式的附件或連結
  - 利用應用程式之弱點(包括零時差攻擊)

社交工程的各種攻擊方法（1/3）

- 電子郵件隱藏電腦病毒
  - 駭客利用社交工程的概念，將病毒、蠕蟲與惡意程式等隱藏在電子郵件中，這些看似朋友所寄來的郵件，卻是應用社交工程的電子郵件陷阱，例如過去造成重大損害的I LOVE YOU蠕蟲，就是一種利用社交工程散播的電腦病毒
- 網路釣魚
  - 偽裝知名企業或機關單位寄發的電子郵件，通知收件人必須重新驗證密碼或登入某網址輸入個人資料等，這種詐騙稱為網路釣魚。收件人若無小心求證而連結了郵件中的鏈結，可能就下載了惡意程式；或者在假網頁上輸入了帳號密碼或信用卡資料等，造成銀行戶頭被盜領或盜刷等的嚴重後果，這是近年來造成個人與企業極大損害的犯罪手法，而網路釣魚就是一種典型的社交工程攻擊。
  - 偽造網址：http://www.hinet.net ←→ http://www.hinet1.net
  - 偽造網頁：製作與原來完全一樣的頁面，以騙取重要的相關資訊。

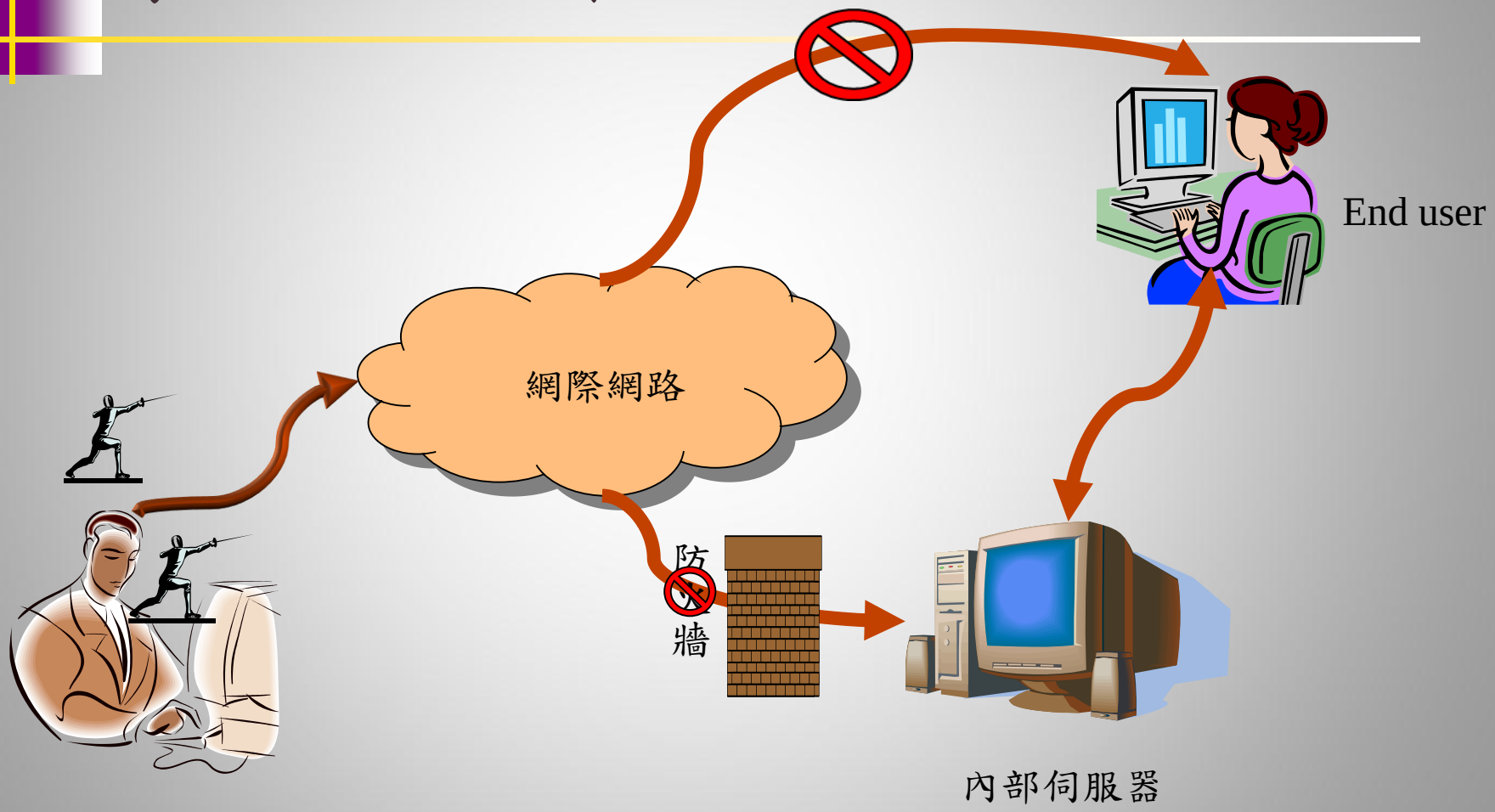
社交工程的各種攻擊方法（2/3）

- 圖片中的惡意程式
  - 明星或色情圖片也是許多惡意程式慣用的社交工程技巧之一，這些都是利用使用者的好奇心來散佈惡意程式，之前Sobig網路病毒出現在某個含有色情內容的網路討論群組，網友點選了其中像是裸照的內容就會感染病毒，而該病毒總共導致了約10億美金的損失。
- 偽裝修補程式
  - 另一種社交工程的欺騙手法，就是偽裝成微軟的修補更新程式，因為一般使用者不會覺得這是來路不明的程式，卻沒有防範社交工程也會利用這個漏洞，而將惡意程式隱藏其中。使用者若安裝了這個檔案，不但不會修補作業系統的任何漏洞，還可能被安裝了遠端竊取資料的木馬程式。

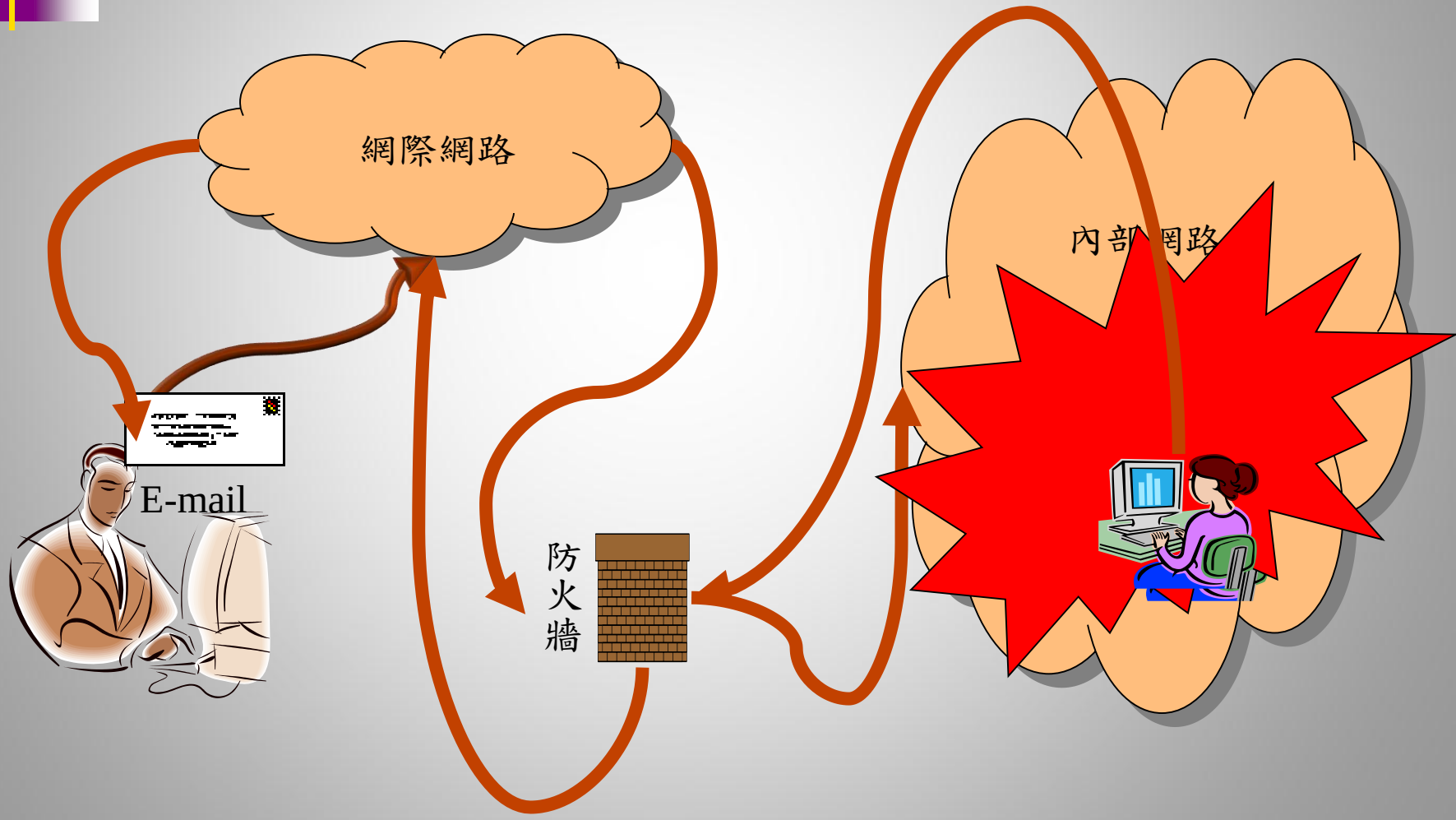
社交工程的各種攻擊方法（3/3）

- 即時通也是社交工程的途徑
  - 近年來，社交工程傳播惡意程式的途徑擴大至即時通訊軟體，手機簡訊也成為另一項值得注意的途徑。
  - LINE免費貼圖詐騙（line ID、FB ID、手機號碼…）http://www.techbang.com/posts/12286
  - **多起網路攻擊以露骨情色誘人,受駭者羞於啟齒,疫發不可收拾!**
    - http://blog.trendmicro.com.tw/?p=11424

傳統網路攻擊



現在網路攻擊模式

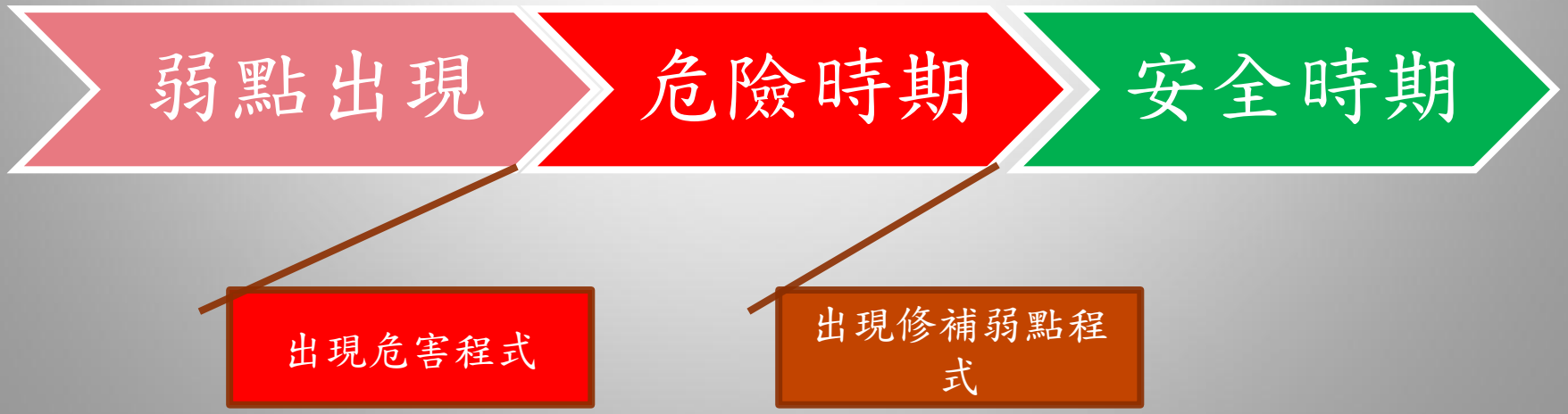


電子郵件社交工程的攻擊步驟

- 有心人設計陷阱或後門程式
- 在電子郵件內放置有害程式或連結
- 將信件寄給特定或不特定對象
- 使用者開啟信件
- 啟動或下載有害程式
- 反向輸出使用者資料（轉眼變成受害者）

軟體弱點與零時差攻擊

- 只要是軟體就可能存在有弱點，未能及修補的話，就可能遭利用被入侵成功。
- 針對軟體弱點未修補前，出現針對弱點的攻擊行為，及稱為「零時差攻擊」。



常見被利用的軟體弱點

- 微軟的作業系統和文書軟體
  - Microsoft office（word）
- 常見的應用軟體
  - Winrar、adobe reader、flash player等軟體

教育部惡意電子郵件社交工程演練
郵件標題

108年上半年度教育部電子郵件社交工程演練標題

編號	信件類別	信件標題
Letter 1	公務類	小 7 無人超商開放第一天　記者實際體驗：結帳只要 10 秒
Letter 2	公務類	東京迪士尼投下 2500 億建新 3 大園區！冰雪奇緣&彼得潘區 2022 年開幕！概念圖預覽
Letter 3	公務類	2018 國民旅遊卡特約商店優惠
Letter 4	公務類	你填問卷，抽週週 Switch 及 百種遊戲片
Letter 5	擬真類	107 年度安全會議紀錄
Letter 6	時事類	2018 最夯燒肉丼排行榜！爆量肉山看了流口水
Letter 7	生活類	107 年度公務人員請假規則修訂說明
Letter 8	財經類	今晨 G7 國際速覽七要聞
Letter 9	旅遊類	公務人員健康檢查之醫院有何規定？
Letter 10	健康類	政府內部控制制度設計原則新規範

108年下半年度教育部電子郵件社交工程演練標題

編號	信件類別	信件標題
Letter 1	公務類	【公文】檢送本部第 952 次（擴大）部務會報紀錄 1 份，請查照辦理
Letter 2	擬真類	108 年下半年資訊安全教育訓練，請尚未參訓之同仁盡速報名
Letter 3	公務類	公文 e 系統維護公告，具時效之公文請提前處理
Letter 4	公務類	最新公告民國 109 年辦公日曆表搶先看
Letter 5	擬真類	轉知：「2019 資通訊網路安全實務強化研討會」意見回饋抽獎活動
Letter 6	公務類	108 年公教人員健檢辦法
Letter 7	生活類	洗牙通知
Letter 8	擬真類	電信費用入賬通知
Letter 9	學術類	民國 108 年環境教育與交流活動
Letter 10	公務類	檢送 108 年度第 6 次處務會議紀錄乙份，請依會議裁示事項辦理

教育部電子郵件社交工程演練案例

公教人員年終工作獎金發給注意事項

公務員懲戒新制實施　處罰爛公務員多三把刀

from: 市政府人事處(lawallspxuiher@hotmail.com)

subject: 檢送108年度第6次處務會議紀錄乙份，請依會議教示事項辦理

from: 國際處理組(internatialtrsns2t3@yahoo.com.tw)

subject: 民國108年環境教育與交流活動

attachment: 環保吸管的挑選方法.doc

您好：
本郵件為教育部電子郵件社交工程演練信件，當您開啟時表示您的警覺性稍有不足。
若駭客使用此信件內容，可能已成功引誘您開啟信件並植入後門程式或病毒。
提醒您應避免開啟與您非信任往來之信件，並注意確認寄件者來源。

教育部資訊及科技教育司　敬上

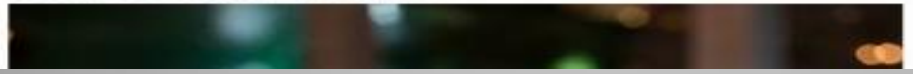
環保吸管怎麼選才好？材質比一比

為了海龜，就像為了極地的飢餓北極熊，我們願意停止浪費，思考更環保、節能的生活，然而依著我正視現實的使用情形，畢竟好用才會多用，光是理想沒有用。

就像是海龜影片之後，台灣的各種環保吸管跟著大賣，可是買了之後真正持續使用的卻不多，因為這些使用上的問題依舊存在：

「帶出去不方便洗」、「難時想買飲料但忘記帶」、「沒有斜口很難插」、「玻璃容易打破」

環保吸管的挑選方法.....



108年度電子郵件社交工程演練結果

	開啟信件	點選連結
合格標準(低於)	10%	6%
清華大學第一次演練結果	10%	8%
清華大學第二次演練結果	0%	0%

1. 清華大學每次演練受測人員共100名（含一、二級行政主管）。
2. 教育部每年度進行兩次電子郵件社交工程演練。

社交工程的防護工作（1/4）

- 作業系統更新
- 應用軟體更新
- 防毒軟體、個人防火牆
- 調整收信軟體的部分設定
- 熟悉所使用軟體基本設定
- 改變使用習慣

社交工程的防護工作（2/4）

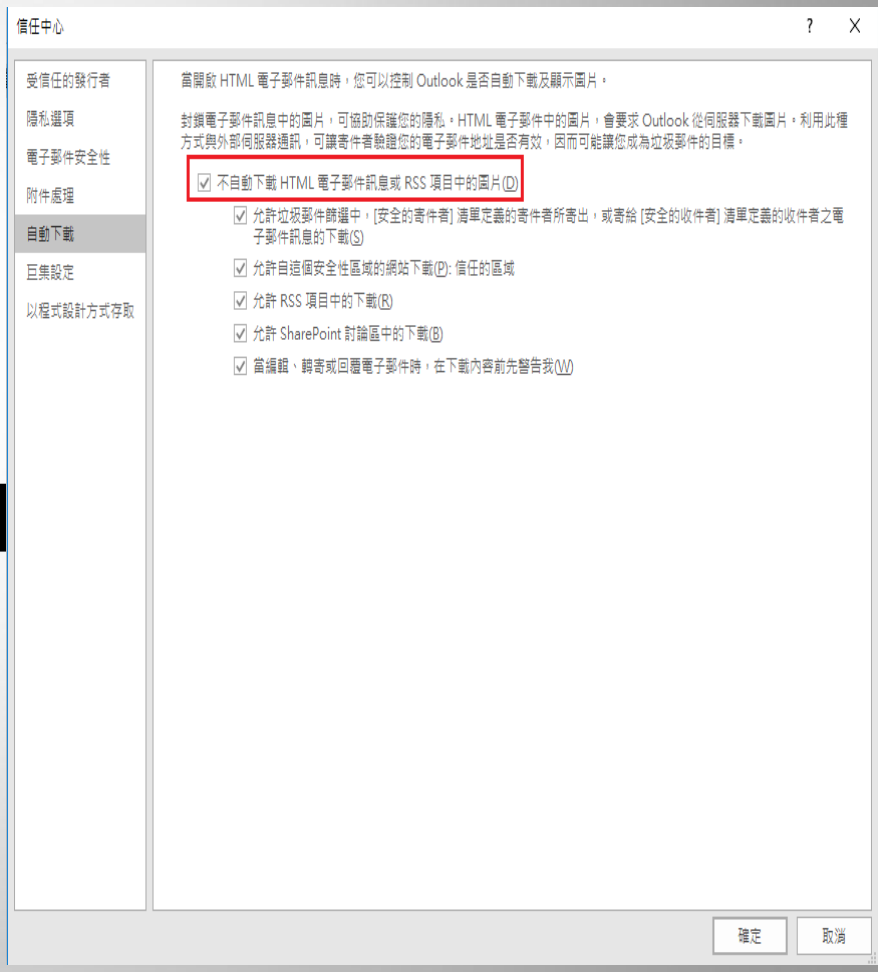
- 作業軟體更新
  - 設定自動更新 microsoft update
- 應用軟體更新
  - Adobe reader…等軟體
- 安裝防毒軟體、個人防火牆並更新病毒碼
  - 卡巴斯基、賽門鐵克、Definder

社交工程的防護工作（3/4）

- 變更看信軟體的設定，提高安全性
  - 不自動下載圖檔
    - Outlook 2019
    - live mail
  - 關閉信件預覽功能
    - Outlook 2019
    - live mail
  - 以純文字開啟信件
    - Outlook 2019
    - live mail

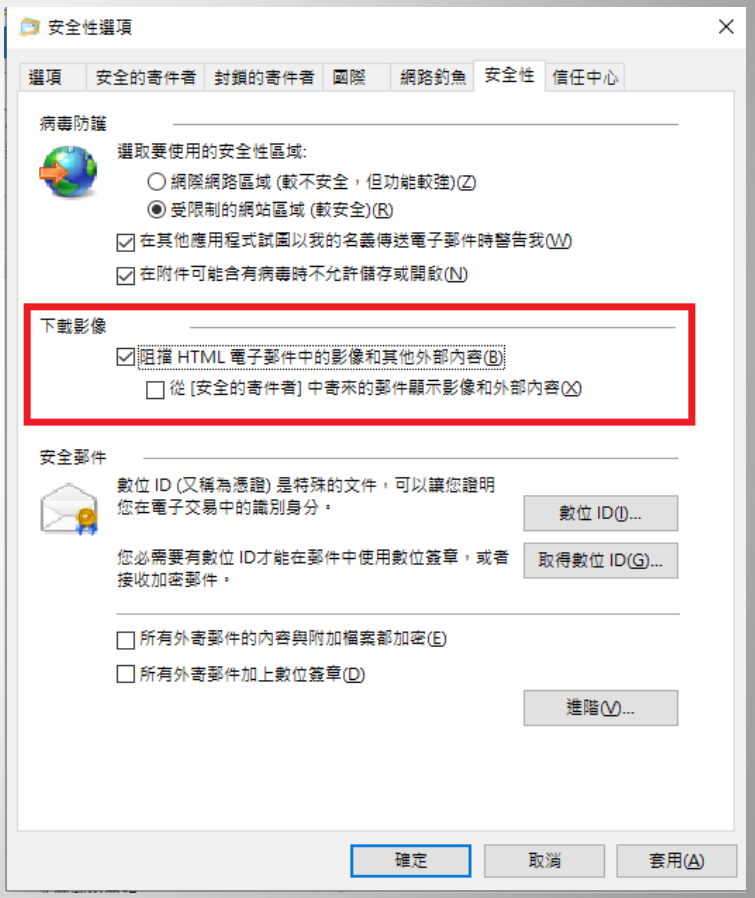
Outlook 2019

- 開啟outlook 2019
- 選取【檔案】
- 選取【選項】
- 選擇【信任中心】
- 點選【信任中心設定】
- 選取【自動下載】
- 將【不自動下載HTML電子郵件訊息或RSS項目中的圖片】打勾



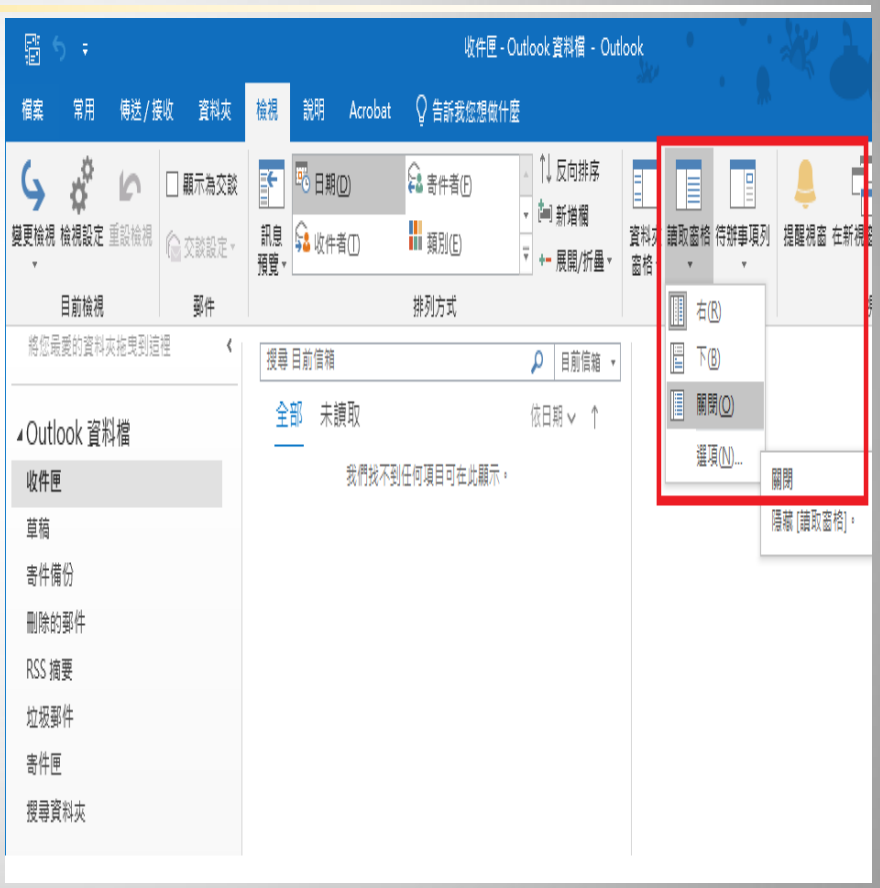
live mail

- 開啟 live mail
- 選取【檔案】
- 選取【選項】
- 選取【安全性選項】
- 選取【安全性】
- 將【阻擋HTML電子郵件中的圖片和其他外部內容】打勾



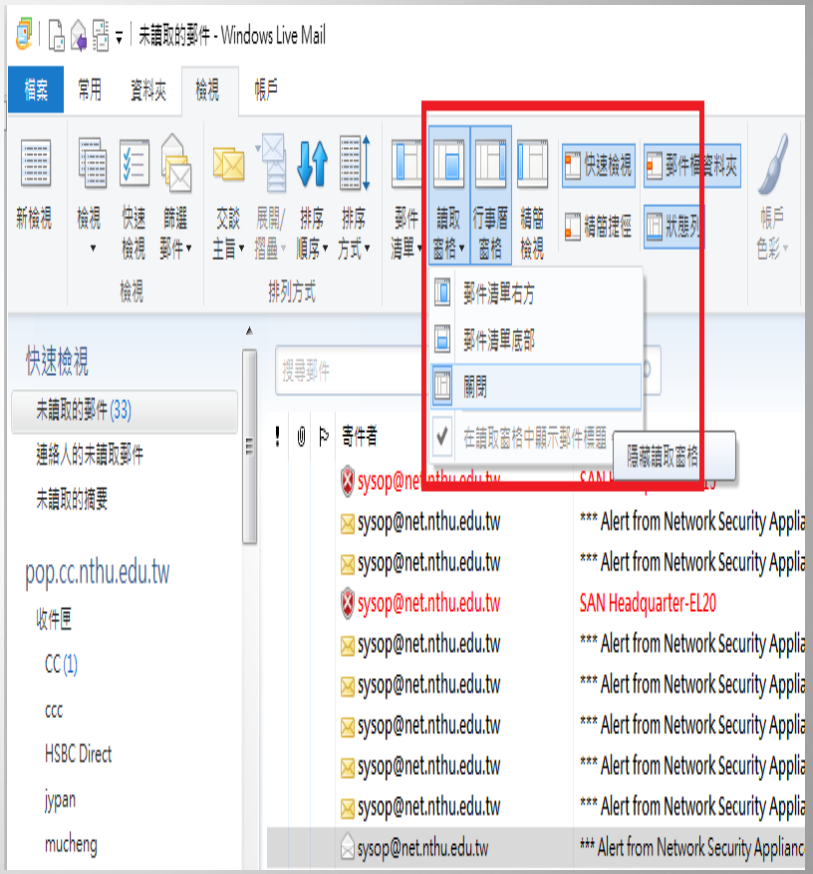
outlook 2019

- 開啟outlook 2019
- 選取【檢視】
- 選取【讀取窗格】
- 選擇【關閉】



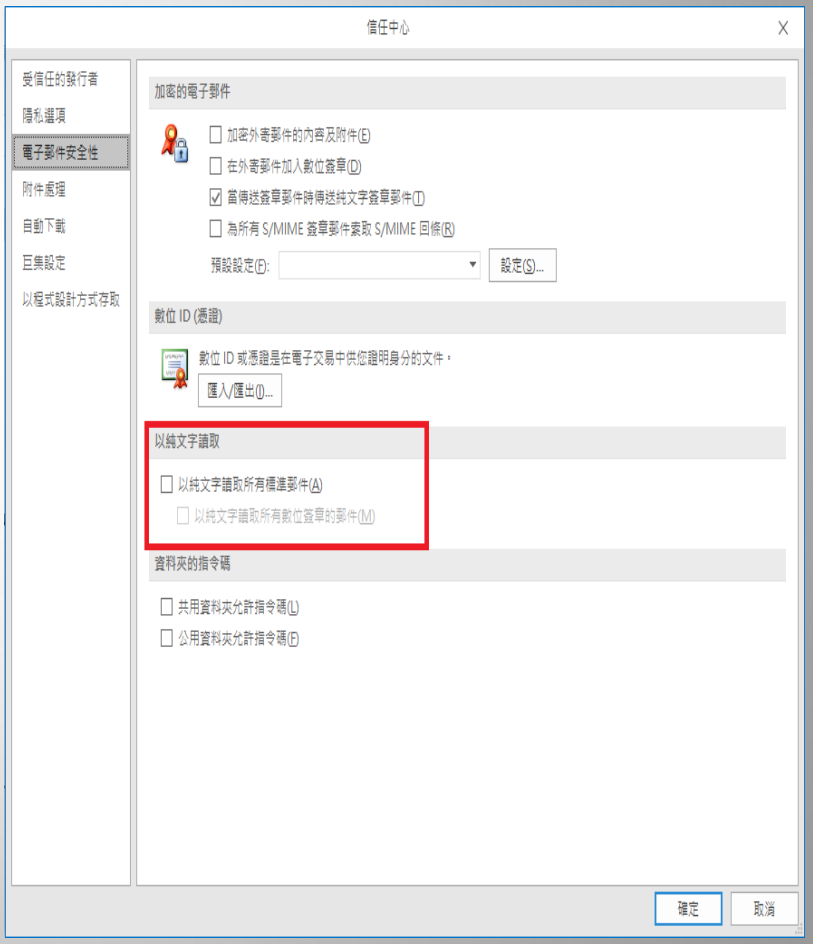
live mail

- 開啟 live mail
- 選取【檢視】
- 選取【讀取窗格】
- 選取【關閉】



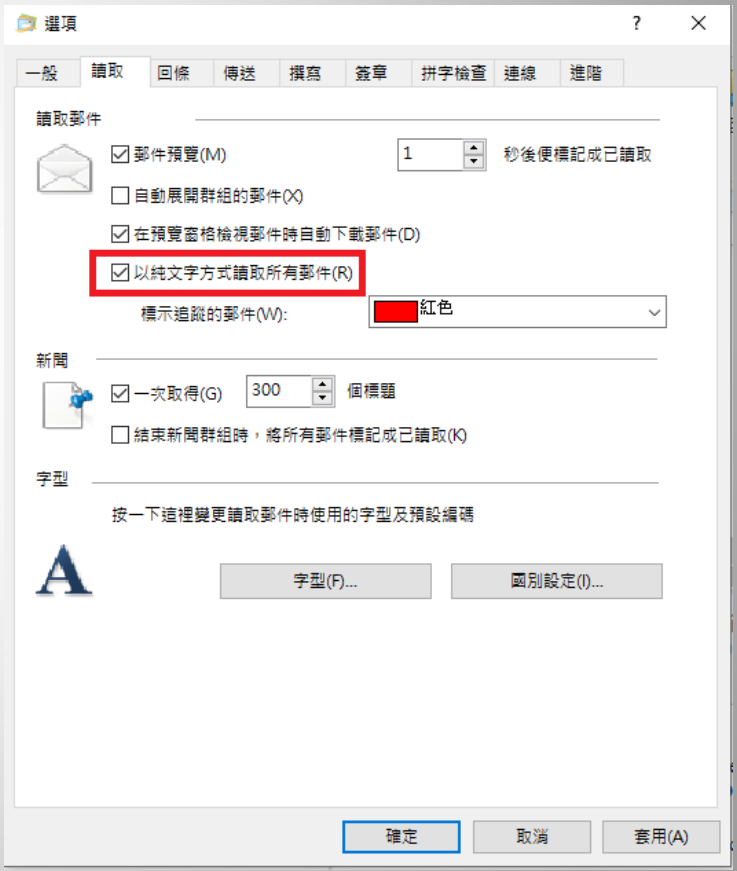
Outlook 2019

- 開啟outlook 2019
- 選取【檔案】
- 選取【選項】
- 選擇【信任中心】
- 點選【信任中心設定】
- 選擇【電子郵件安全性】
- 將【以純文字讀取所有標準郵件】打勾



live mail

- 開啟 live mail
- 選取【檔案】
- 選取【選項】
- 選取【郵件】
- 選取【讀取】
- 將【以純文字中讀取所有郵件】打勾



社交工程的防護工作（4/4）

- 改變使用電子郵件的習慣
  - 查明信件的來源
    - 信件可由mail header查出所經的伺服器
  - 釐清寄件者身分
    - 以電話向寄件者確認
    - 郵件驗證機制
    - 附件加密
    - …

Mail header

Retu
X-Or
Deliv
Rece

Rece

Rece

From
To: Y

Return-Path: <vipmember@infoarray.tw>
X-Original-To: OOO@mx.nthu.edu.tw
Delivered-To: OOO@mx.nthu.edu.tw
Received: from cp1.oz.nthu.edu.tw (cp1.oz.nthu.edu.tw [140.114.63.141])
by cc.nthu.edu.tw (Postfix) with ESMTP id AA6BA56C76
for <ptlin@cc.nthu.edu.tw>; Thu, 2 Jul 2009 13:56:42 +0800 (CST)
parts
Received: from mail.communicatearea.tw [(210.67.251.27)] by cp6.oz.nthu.edu.tw
(envelope-from <vipmember@infoarray.tw>)
(NTHUCCC AntiSPAM Mail Server with TLS)
with ESMTP id 577192816; Mon, 18 May 2009 06:55:06 +0800
Received: from mailsystem ([192.168.255.100])
by mail.communicatearea.tw (8.13.8/8.13.8) with ESMTP id n4HMs4w7018426
for <OOO@mx.nthu.edu.tw>; Mon, 18 May 2009 06:54:06 +0800
X-ssage-ID: <7141115.1242600903628.JavaMail.SYSTEM@mailsystem>
Date: Mon, 18 May 2009 06:55:03 +0800 (CST)

結論

- 兩不看
  - 來源不明的信不看
  - 不認識寄件者不看
- 不衝動
  - 對於自己有興趣、有吸引力....等信件

網際網路服務介紹

- 服務狀態即時查詢
- 信箱取信記錄查詢
- 信箱檢測
- 寄信記錄查詢
- 寄信白名單服務

虎三小之童話變奏 社交工程
電子郵件社交工程宣導影片

報告完畢

謝謝