# 國立中興大學

## 電子郵件暨駭客社交工程攻擊與防禦

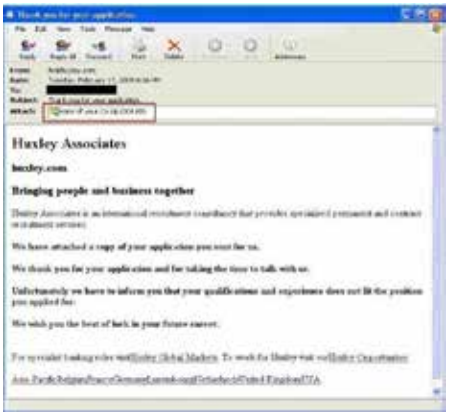
Davies Wang
5,2013

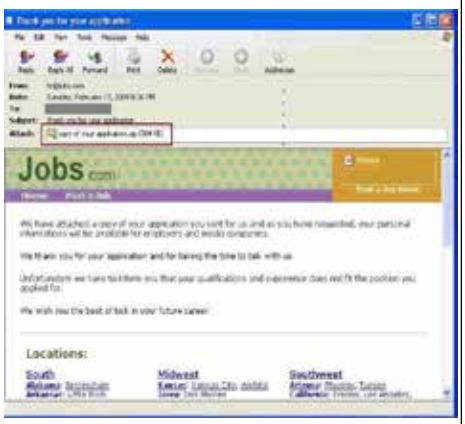
## 課程大綱

- 詐騙電子郵件之案例分析
- 社交工程與相關防護方式
- 電子郵件使用安全管理

# 案例分析：駭客也在求職網找工作

* 下面電子郵件樣本是冒充jobs.com發送的信件：
  * 信件來源看似來自人力資源部門:hr@jobs.com
    信件標題是：「Thank you for your application」
    附件是：copy of your application.zip




# 案例分析：引毒上身？五成網友主動下載有毒影音檔、電子郵件

* 記者蘇湘雲／台北報導
* 總是抱怨網路毒駭事件層出不窮的使用者聽到以下消息，可能要先檢討自己為何如此「手癢」囉！入口網站最新調查顯示，網路中毒原因的前三名分別為「下載有毒的音樂或影音檔案」（27.6%）、「帳號被盜」（26.7%）及「收到夾帶有毒檔案和連結的電子郵件」（24.2%），除了帳號被盜，有五成 以上的網友都是「主動被駭」，主因來至網路安全知識的不足，而誤入「毒」徑。
* 網友最容易點選「跟搜尋結果相關的網站」（42.3%）及「好友寄的信件或訊息」（29%）而上了有毒程式的釣鉤，誤入電腦被駭的危機。而另外依序還有「免費試玩或下載」（13.9%）、「火辣性感圖」（7.3%）及「折扣好康」（5.7%）等誘人資訊也會讓網友忍不住點選。
  透過交叉分析也發現有趣的現象，會被「折扣好康」內容吸引的女性網友為男性的三倍，而「火辣性感圖」的內容吸引者則大多數為男性網友。

# 案例分析：來自資通安全會報技服中心的通知

- 近日國家資通安全會報技術服務中心發現，有不明駭客假冒國家資通安全會報技術服務中心之客戶服務信箱名義發送含有惡意程式之電子郵件。
- 目前已知該假冒信件訊息如下:
  - 寄件者：service@icst.org.tw
  - 主旨為「W32.Timeserv@mm 病毒通告」
  - 附件有3 筆名稱分別為「安全防護.ppt」、「病毒原理.ppt」、「解決方案列表.xls」。


# 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。
  - 以人為本騙術為主
  - 技術門檻較低
  - 貪心：撿便宜的個性
  - 好奇：探索感興趣的事務
  - 缺乏警覺：有那麼嚴重嗎？

# 網路釣魚

- 網路釣魚(Phishing)是網路上在常見的社交工程，特別是利用Email來欺騙，對於此類攻擊的最佳對應方法就是在預覽前就刪除所有類似的郵件，如此亦可同時避免會在背景觸發不良程式的惡意郵件攻擊。
- 只要使用者警覺性不足，點選網頁連結或是開啟來路不明郵件的附加檔案，都可能被植入惡意程式。
- 當收到不尋常或太好康的訊息時，應思考訊息內容的可行性，千萬不要下載附件或是連結網頁，並依循資安通報管道進行通報。

# 網路釣魚方法

- 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l
- 或用數字0來取代英文O
- xxx.com.tw 或 xxx.com
- 發E-mail、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

# 網路釣魚之媒介

- 搜尋引擎與入口網站
  - Google
  - Yahoo
- IM軟體
  - MSN
  - Skype
  - ICQ
  - Facebook
- E-Mail
- 手機簡訊
- 廣告

# 網路釣魚目的

- 廣告目的(不斷開啟惡意廣告)
- 攻擊目的(植入後門程式)
- 金錢目的(詐騙行為)
  - 花旗銀行(mail)
  - 旅遊網站
  - 拍賣網站
- 竊取帳號密碼與個人資料

# IM詐騙

# 電腦幫忙記密碼 小心被駭偷光光

* **資安案例**
* 帳號密碼太多太難記，想靠電腦記憶省腦力，事實上電腦不一定比人腦可靠，專家指出，讓瀏覽器把密碼記下來，一旦電腦遭入侵，重要的帳號密碼就很容易被偷走，建議民眾除了時常更新密碼外，也不要把所有的帳號密碼存在同一個檔案裡。有沒有算過一整天使用電腦要輸入幾組帳號密碼？打開電腦，收發電子郵件、啟動即時通、進入部落格甚至是上網轉帳，一般人少說有四組以上的帳號密碼，更別談是電腦重度使用者，要靠腦袋瓜記住這麼多數字，光想就暈頭轉向，不少人為了方便使用，乾脆讓電腦幫忙記住密碼，不過專家提醒，電腦被入侵，最大的損失通常是帳號密碼被竊取，而讓伺服器記憶密碼，其實藏有潛在風險。
* **資安威脅類型：**人員疏失

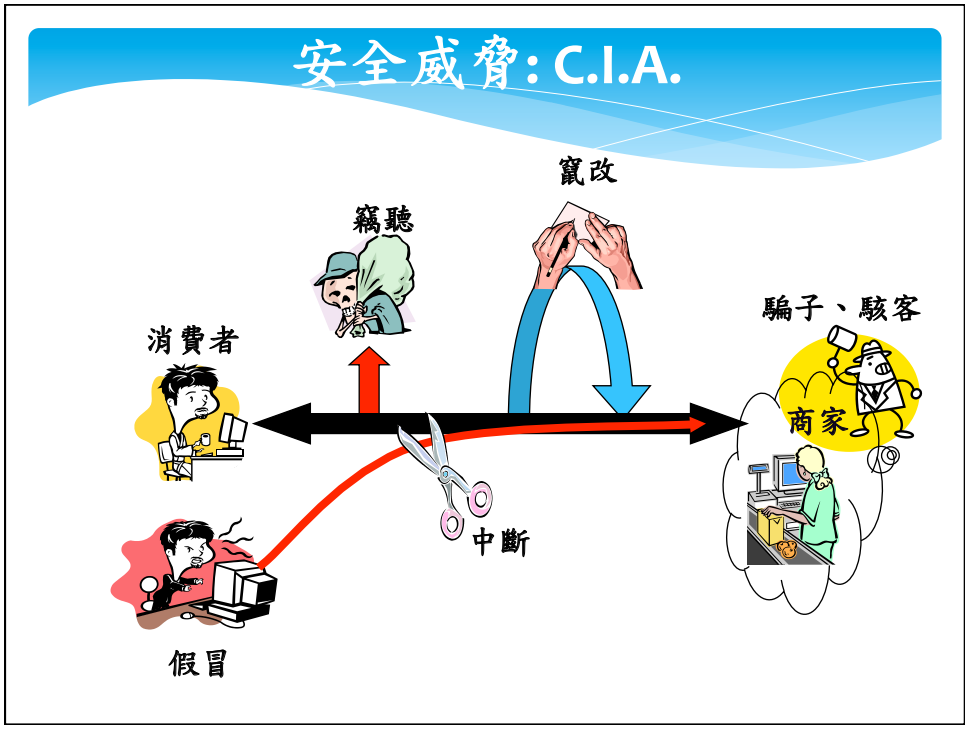
  **Cookies可以提供哪些資料?**

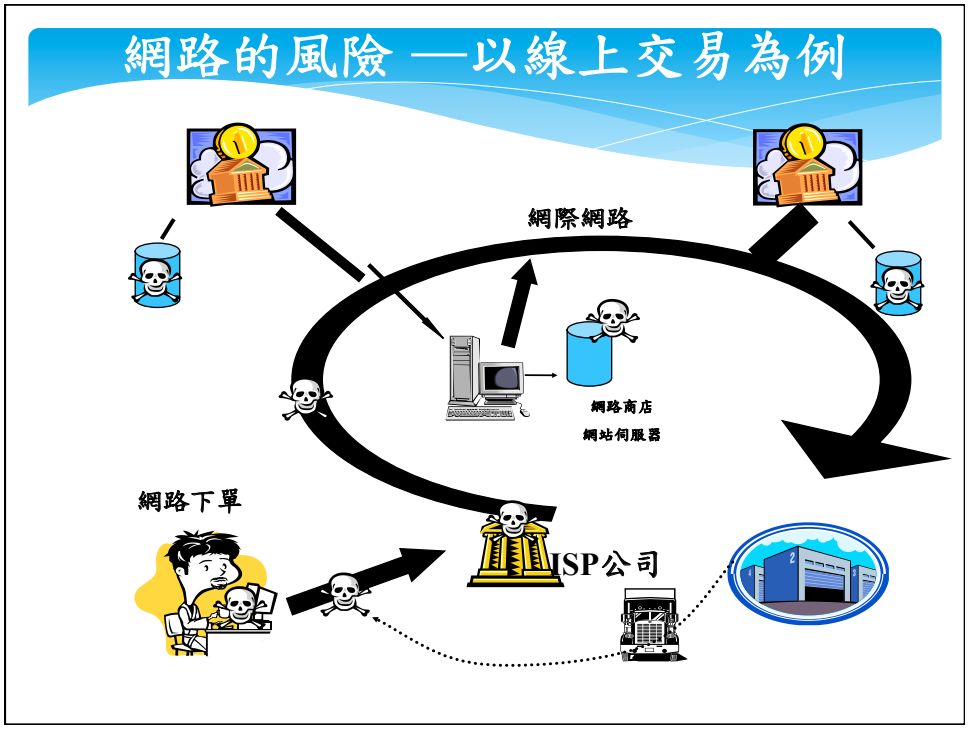

資料來源：中廣新聞網

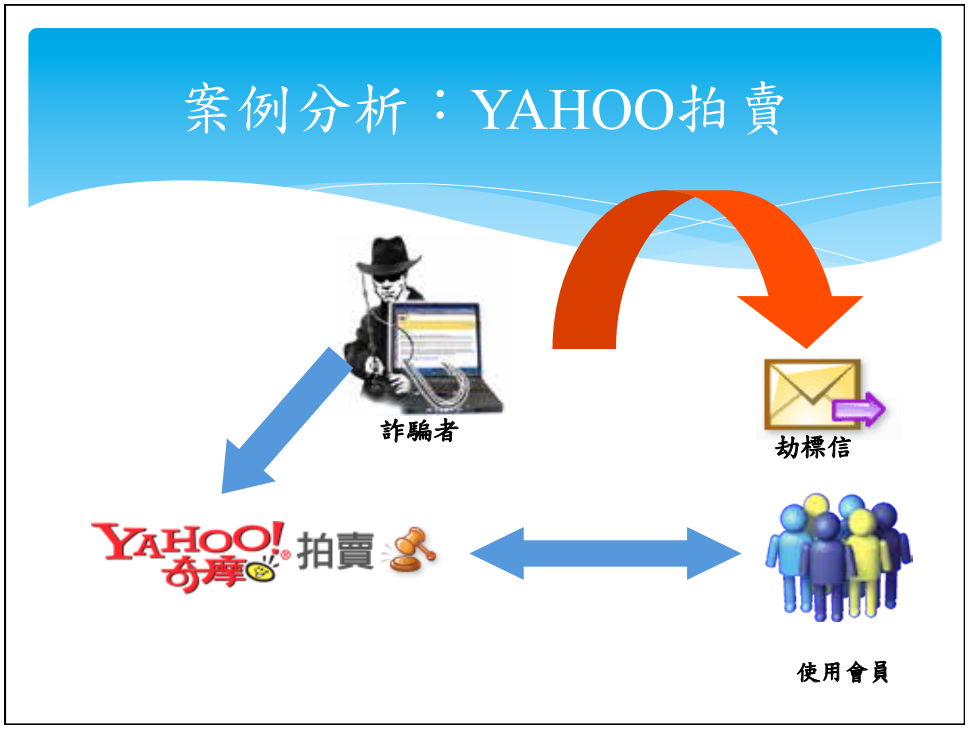
# 「我的最愛」是釣魚台?

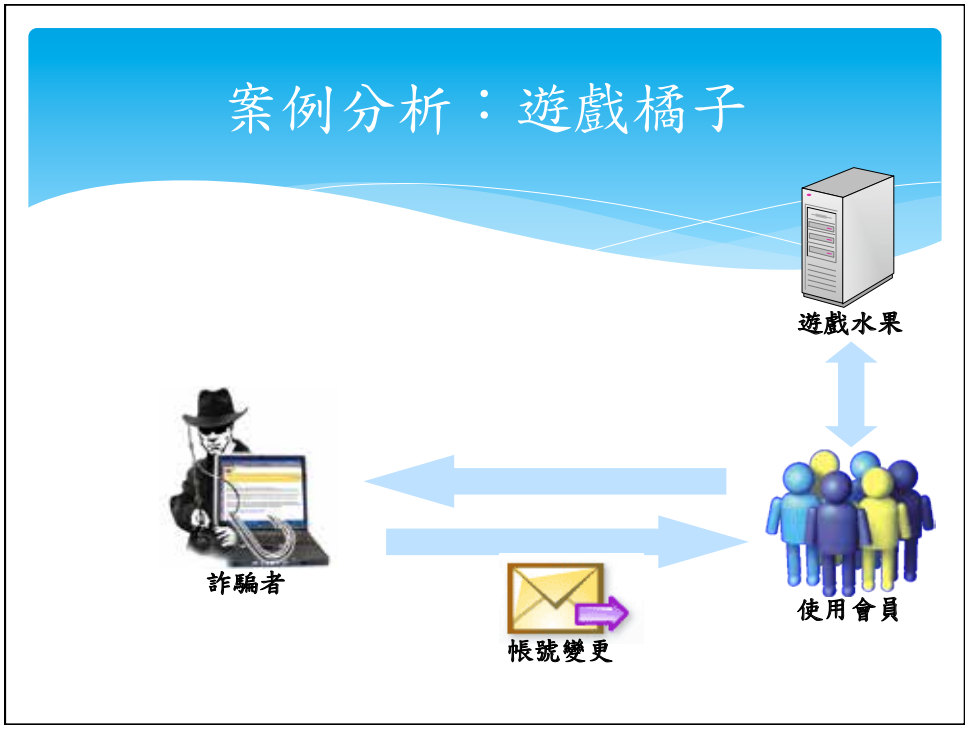
- 合作金庫www.tcb**c**-bank.com.tw/
- 土地銀行www.**1**andbank.com.tw/
- 中國商銀www.**1**cbc.com.tw/

# 網路騙術何其多?真假網站


安全威脅: C.I.A.
竄改
竊聽
消費者
騙子、駭客
商家
中斷
假冒


網路的風險 —以線上交易為例
網際網路
網路商店
網站伺服器
網路下單
ISP公司


案例分析：YAHOO拍賣
詐騙者
劫標信
YAHOO!奇摩 拍賣
使用會員


案例分析：遊戲橘子
遊戲水果
詐騙者
使用會員
帳號變更

# 案例分析：偽冒網站


# 案例分析：垃圾郵件

## 案例分析：來自資通安全會報技服中心的通知(續)

- 事件說明
  - 此事件為一起「零時差攻擊」（Zero-day Attack），因此附檔使用的弱點所使用的未公開的 Office 漏洞目前尚無更新程式可修補。
  - 經調查，駭客大量寄發經特殊設計的電子郵件，顯示此次大規模入侵事件並非個案。
- 解決之道
  - 若有收到類似不明信件，請勿開啟以避免其他攻擊，發生造成更嚴重之後果。

## 同仁對於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（寄件者或資訊中心）。

# 判斷網路釣魚郵件方式

- 發信人的名稱或郵件地址
  - 是否有異常？需確認發信者的身分
- 電子郵件的主旨與內容
  - 與本身的工作、業務是否有關連
- 網頁連結或夾帶附件檔案是否可疑
  - 郵件內異常網址連結判斷
    - www.microsoft-mis.com
    - www.hinet1.net , www-hinet.net
    - www.paper-pchome.com , www.pchorne.com
    - 使用不明IP 代替URL（如：http://220.33.444.12/）

# 判斷網路釣魚郵件方式

- 附加檔案之檢查
  - 與接收者的日常工作是否有關
  - 往往帶有惡意攻擊碼的檔案不易察覺
  - 常見病毒附件檔案副檔名
    （.bat、.pif、.exe、.zip、.src、.cmd、.rar等）
- 對於切身相關的電子郵件，若內含威脅、利誘、警告、提示等訊息內容，先思考後再行動作，應考慮詐騙之可能性

# 防範惡意程式與詐騙

- 個人資訊勿隨意登錄於不明網站
  - E-mail 管理
    - 區分公司及個人使用之信箱
    - 在外登錄註冊之信箱，容易收到許多垃圾郵件，使用時務必小心
    - 不回覆來源不明之郵件
  - 定期安檢作業
    - 即時更新軟體修補程式
    - 即時更新防毒軟體及病毒碼
    - 經常對系統進行檢測
  - 實體隔離
    - 機敏資料應於實體隔離主機上作業

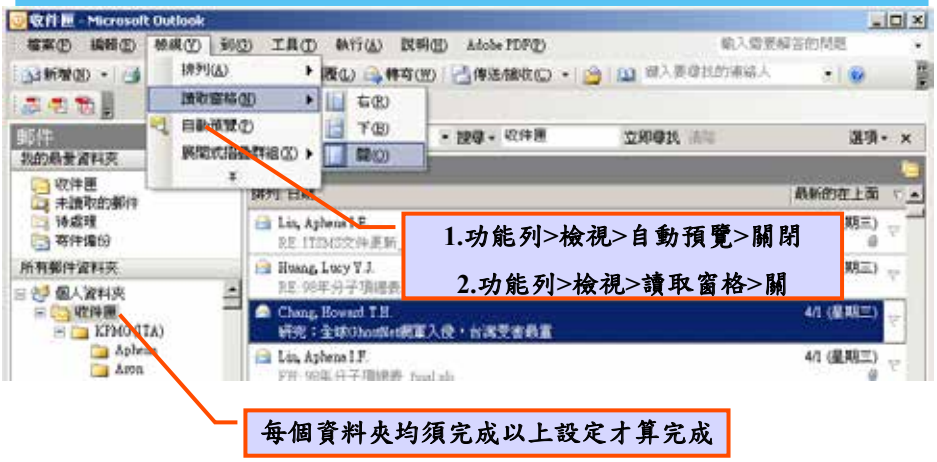
# 同仁對於可疑電子郵件應有警覺性

- 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(寄件者或資訊科)

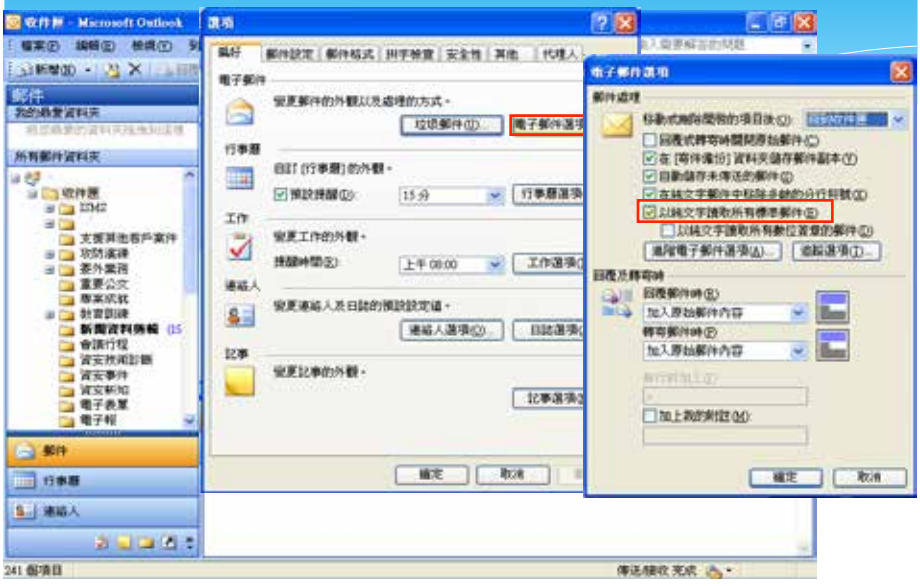
# 電子郵件安全防制措施

- 同仁之電子郵件應「關閉預覽郵件」設定。
- 同仁之電子郵件應設定為「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。
- 如發現為不明來源或疑似網路釣魚之郵件應直接刪除。
- 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單位查證。
- 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
- 非必要不設自動回覆
- 不隨意留下郵件地址予他人
- 注意陌生之寄件者
- 了解組織傳送郵件規定

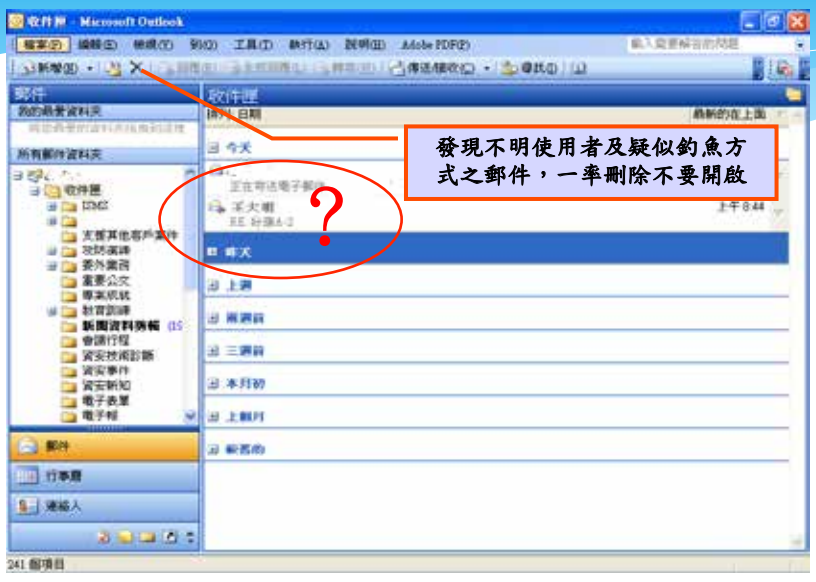
# 一、Outlook取消郵件預覽



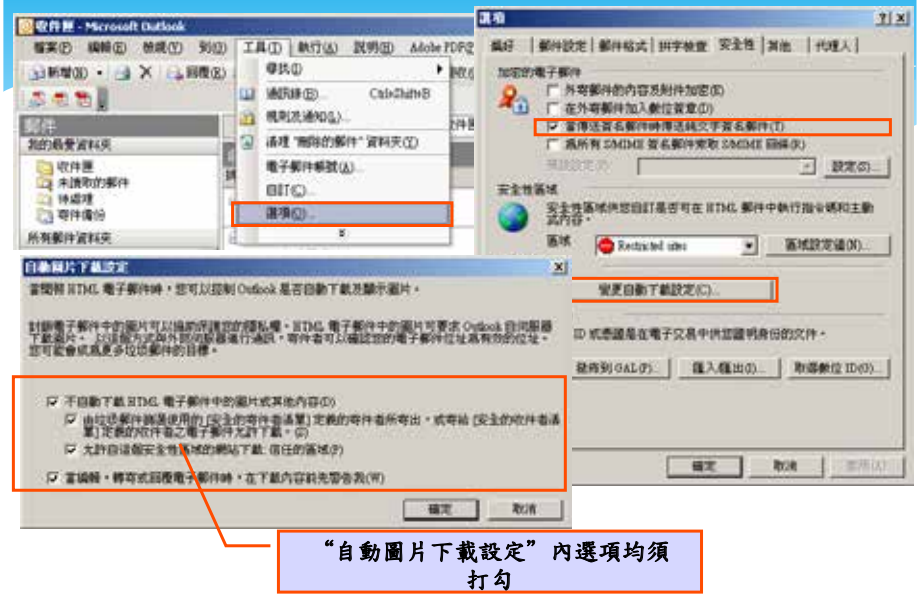
## 二、Outlook設定純文字模式開啟郵件



## 三、Outlook刪除不明來源郵件

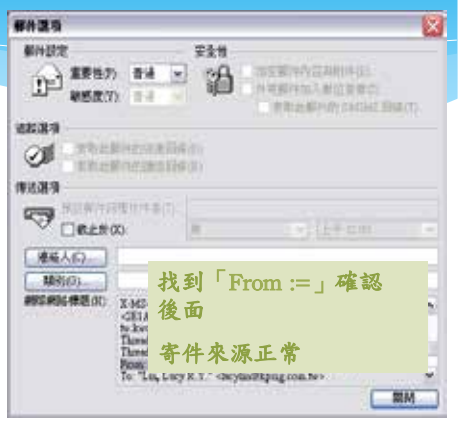


## 四、設定阻擋HTML電子郵件中的圖片

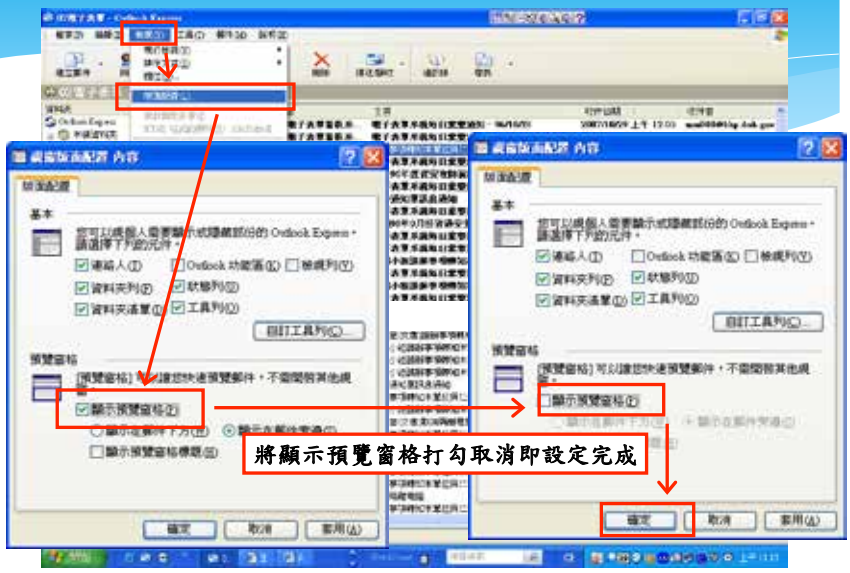



## 五、Outlook確定發信者電子郵件帳號

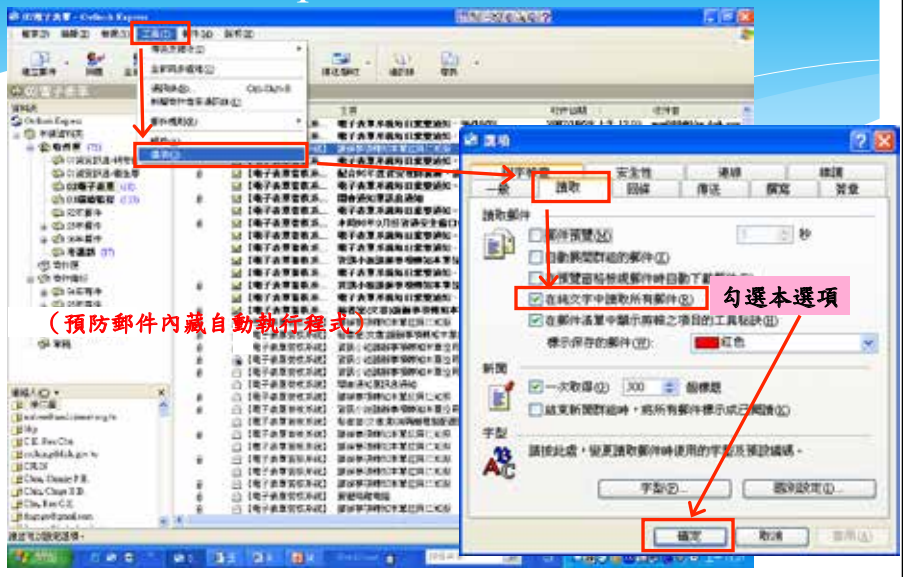
# 判斷郵件真偽


# 一、Outlook Express關閉預覽視窗設定

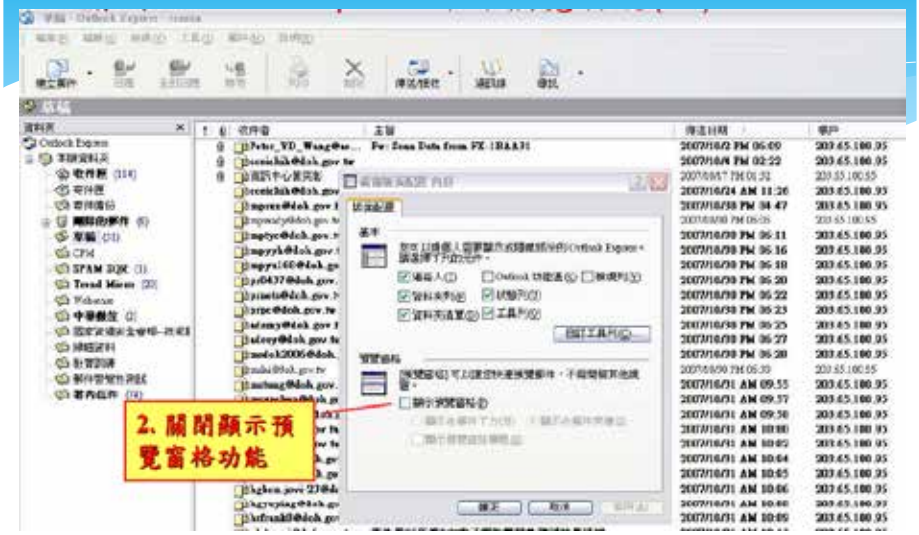


## 二、Outlook Express以純文字模式開啟郵件

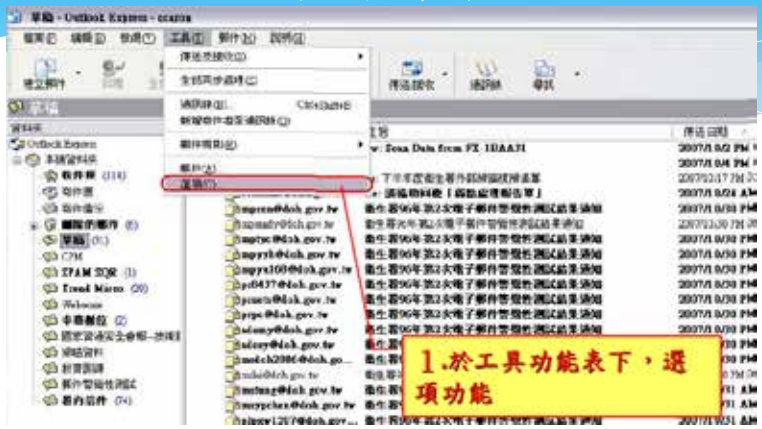



## 三、關閉Outlook Express郵件預覽功能

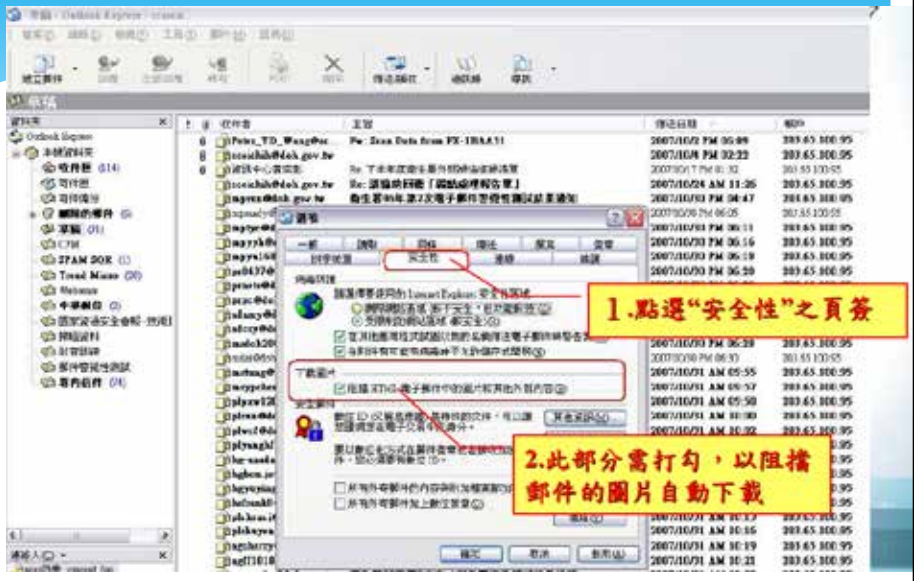
## 三、關閉Outlook Express郵件預覽功能



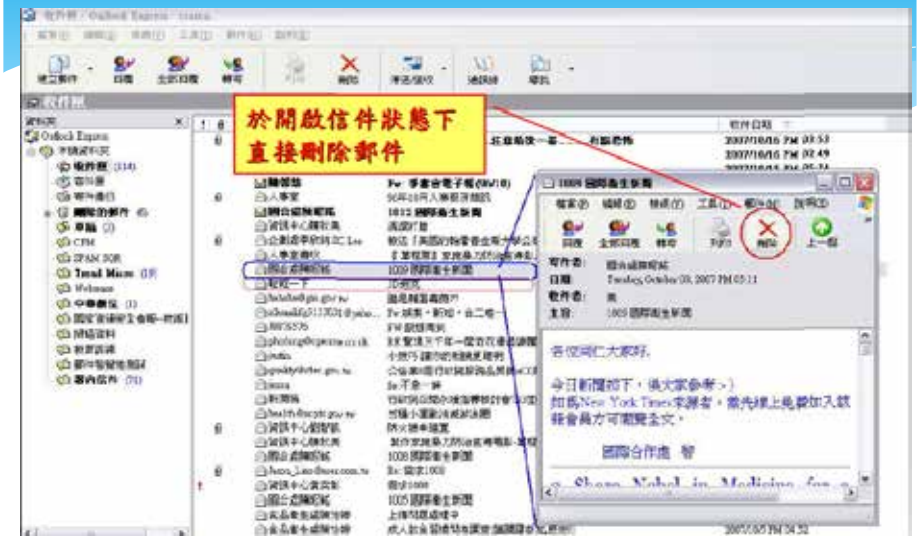

## 四、設定Outlook Express阻擋電子郵件中的圖片



## 四、設定Outlook Express阻擋電子郵件中的圖片(續)




## Outlook及Outlook Express操作注意




電子郵件社交工程手法
詐騙者
惡意網站
機密資料
帳號/密碼
跳板主機
使用者

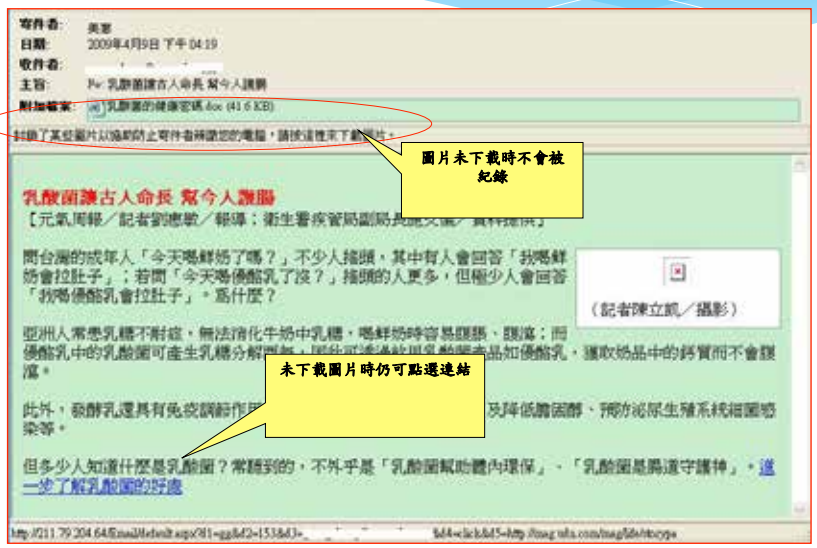

惡意郵件攻擊
資料來源：法務部全球資訊網
好康報、養生保健、休閒娛樂、公務相關、美食、八卦新聞...

# 測試郵件清單

| 郵件 | 郵件種類 | 郵件標題 | 寄件者 |
|---|---|---|---|
| 1 | 趣味遊戲 | Fw:台灣Facebook農田滿種第一人，share農民幣密技 | 婷婷<tintin336@yahoo.com.tw> |
| 2 | 政治 | 李家同：免試入學，窮人孩子出頭不易 | 教改聯誼會<callcenter@tw.standardchartered.com> |
| 3 | 衛生保健 | Re:多吃B群吧，新聞說國人維生素B群最缺 | 菁菁<annie0908@mail2000.com.tw> |
| 4 | 趣味遊戲 | fw:豬認「狗」當媽！瘋狂吸奶 狗媽媽爆瘦10公斤 | 蕙玲<linlin@npm.gov.tw> |
| 5 | 情色 | 林嘉綺代言電玩演出，驗奧女神：最後一次裸露 | 電玩週報<game@ms66.url.com.tw> |
| 6 | 新聞時事 | 像世界末日般，雪梨沙塵染紅歌劇院圖集 | weather<weather@yam.com> |
| 7 | 旅遊休閒 | 日月潭纜車啟用，旅遊Passport搶手 | 雄貓旅行社<travel_cat@pie.com.tw> |
| 8 | 新聞時事 | 汽車貨物稅減徵3萬最後倒數，腳步加快 | 汽車雜誌<car@ferrari.com> |
| 9 | 網路新知 | 青年安心成家方案，逾5成買前不知道 | 永慶房仲網<customer@sinyi.com.tw> |
| 10 | 八卦 | 連父親都瞞? 林志玲爸爸要當阿公卻不知?! | 阿霞<info@log.1-apple.com.tw> |

# 網頁型測試郵件範例

# 釣魚郵件記錄方式




# 防範惡意電子郵件使用者防護

* 停－使用任何電子郵件軟體前，須先確認以下設定
  * 是否已安裝防毒軟體並確實更新病毒碼
  * 取消郵件預覽功能(outlook express/檢視/版面配置/預覽窗格，不要勾選顯示預覽窗格的設定)
  * 儘量使用純文字模式開啟信件(outlook express/工具/選項/讀取/讀取郵件，☑在純文字中讀取所有郵件)
* 看－收到信件後必須注意
  * 信件主旨是否與本身業務相關
  * 開啟信件前須先確認信件來源，否則建議刪除
* 聽－若懷疑信件來源必須進行確認
  * 透過電話或電子郵件向寄件人確認信件真偽

## 改善個人習慣

- 不要瀏覽非工作相關或不信任的網站
- 不要下載安裝未經認可的軟體或程式
- 隨時更新作業系統與應用程式
- 安裝必要的防護軟體
- 不要開啟可疑或非工作相關的信件附檔
- 對任何提到”緊急”或”個人金融”保持懷疑態度
- 對信件有任何一點疑慮千萬不要點選Email裡的超連結
- 不要填寫Email裡有關個人金融資料的表格
- 在網站上輸入信用卡號或個人資料時先確認該網站安全性

## 改善個人習慣(續)

- 不將Email留在任何公開的網頁上
- 不開啟來歷不明之信件
- 不轉寄非必要之信件
- 不回應任何未知的信件
- 安裝防止網路釣魚詐騙的工具軟體
- 經常或定期登入你的網路帳號
- 定期確認你的銀行帳戶、信用卡的交易狀態都正確無異常
- 確認你的瀏覽器、收信軟體、文書軟體及其他程式是最新版本，而且都已更新修補程式
- 自助互助，告知相關單位你發現的網路釣魚事件

## 結論

- 預防重於治療
- 隨時注意更新
- 正確的觀念

## 問題與討論

**聯絡資訊**

**王吉祥 講師暨資深經理**
**+886 970 350 128**
**dvings@gmail.com**