電子社交工程防範

資訊處　　網路管理組　　謝丞智

教育部演練時程

1. 提報演練名單：請於4月13日前提報受測人員之電子郵件帳號，並標記正、副校長及一級主管，演練名單資料請直接以電子郵件方式寄送給教育部資科司。

2. 本部進行第1次集中演練：107年4月。

3. 納入本部演練單位針對開啟惡意郵件或點閱惡意郵件附件內容人員，進行加強宣導：自107年7月至107年 8月上旬。

4. 本部進行第2次集中演練： 107年 9月。

何謂社交工程?

- 社交工程，英文為Social Engineering，是以影響力或說服力來欺騙他人以獲得有用的資訊，這是近年來造成企業或個人極大威脅和損失的駭客攻擊手法。

- 簡單來說「社交工程」，就是詐騙！透過電話、電子郵件等方式偽裝身份誘騙您上勾受騙…

社交工程的各種攻擊方法

- 電話詐騙
- 電子郵件詐騙
- 網路釣魚
- 圖片、網頁內的惡意程式
- 偽裝修補程式
- 即時通（LINE, Facebook Messenger, Skype ,QQ...）

電子郵件攻擊手法

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~時事相關或令人感興趣的郵件內容
- 含有惡意程式的附件
- 利用應用程式之弱點(包括所謂零時差攻擊)
- 是一種並非完全技術性的資訊安全攻擊方式，即使建置技術精良的資安設備或高效能的防護系統，也無法完全防止社交工程攻擊

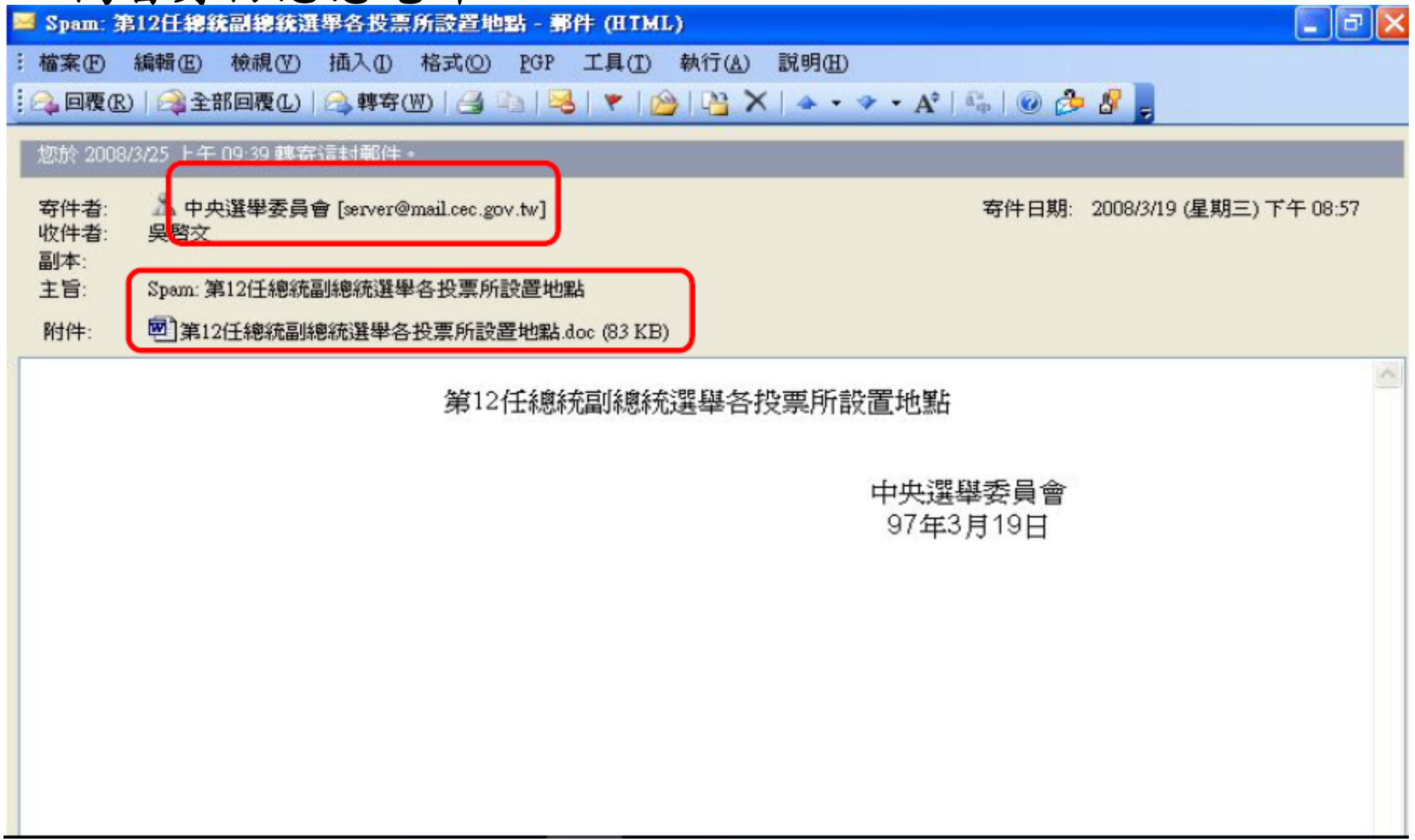
電子郵件攻擊手法

混淆視聽之郵件寄件者

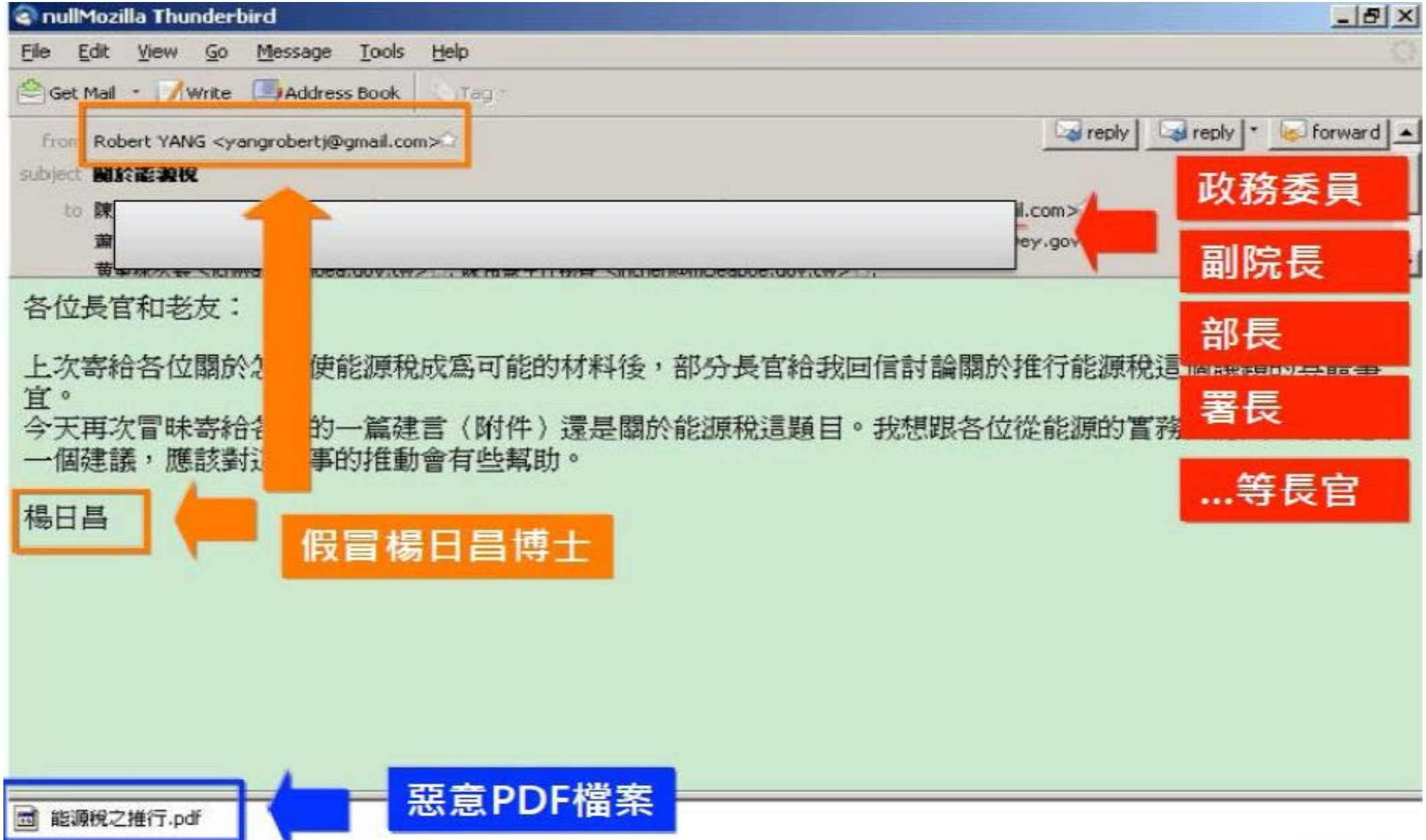
- 偽裝身分(王小明、Alex)
- 偽裝機關(AB銀行、XY商店)
- 偽裝服務(OX論壇電子報、YAHOO新聞)
- 附件夾帶病毒~蠕蟲~木馬程式及殭屍程式等惡意程式
- 郵件本文夾帶惡意連結
- 假冒使用者信任的人，讓使用者相信電子郵件的內容，而去開啟附件或超連結，暗中啟動木馬程式

電子郵件攻擊手法

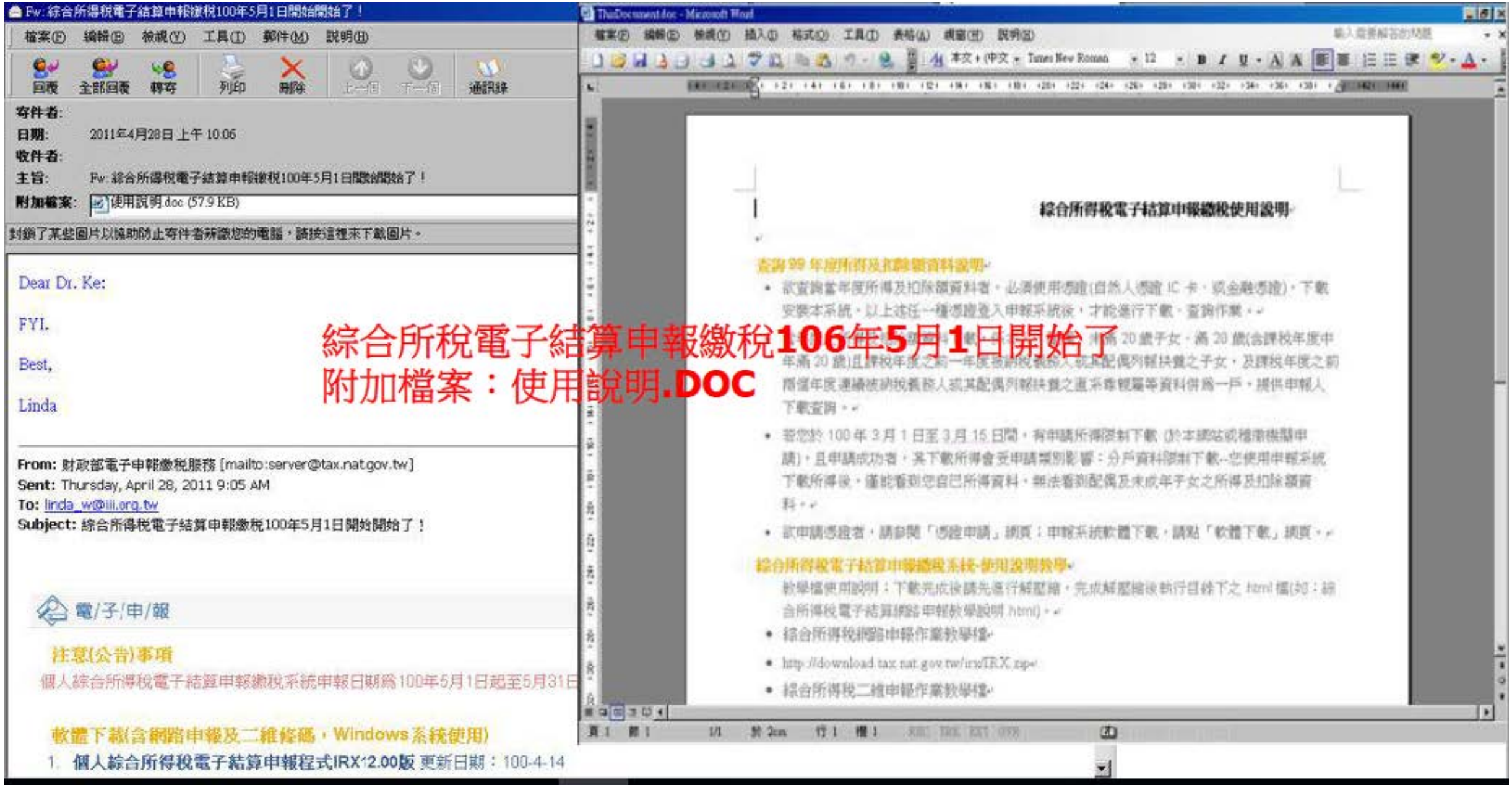
□偽冒身份惡意電郵



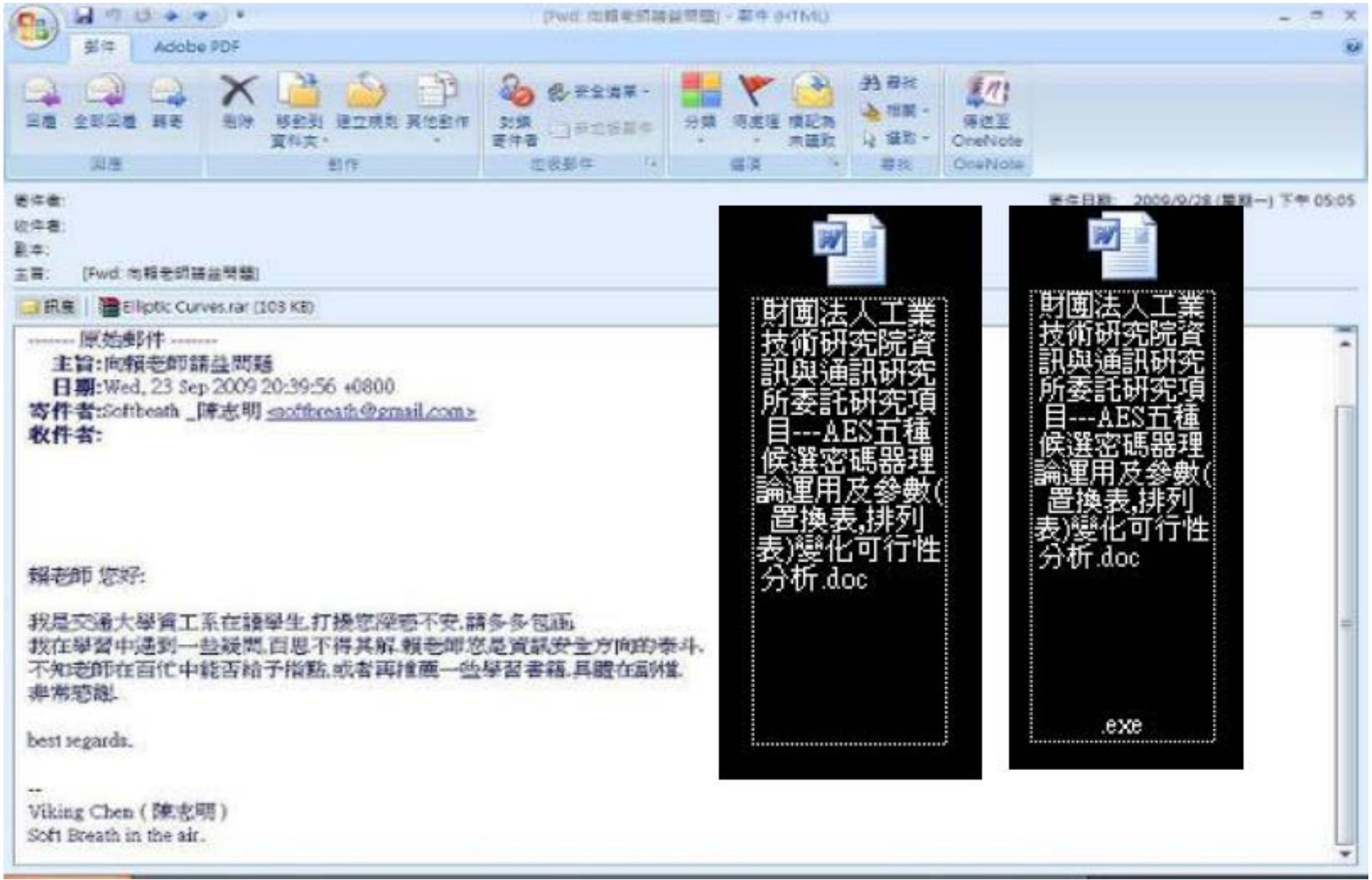
□偽冒身份惡意電郵


nullMozilla Thunderbird
File Edit View Go Message Tools Help
Get Mail Write Address Book Tag
Robert YANG <yangrobertj@gmail.com>
reply reply forward
subject
to
各位長官和老友：
上次寄給各位關於怎使能源稅成爲可能的材料後，部分長官給我回信討論關於推行能源稅這
宜。
今天再次冒昧寄給各的一篇建言（附件）還是關於能源稅這題目。我想跟各位從能源的實務
一個建議，應該對事的推動會有些幫助。
楊日昌
假冒楊日昌博士
政務委員
副院長
部長
署長
...等長官
能源稅之推行.pdf
惡意PDF檔案

□含有惡意程式的附件–偽裝報稅通知訊息



□利用圖示修改與副檔名隱藏方式，引誘使用者開啟



社交工程電子郵件內容

令人緊張或鬆懈防備之郵件主旨

- 關心提醒(請告訴身旁的女性朋友，小心電梯之狼)
- 誇大聳動(世界末日大預言)
- 郵件回覆(RE:會議參考資料)
- 郵件轉寄(FW:簡易規劃日本自助旅行)

工作業務、生活時事等相關或令人感興趣之郵件內容類型

- 政治新聞、特殊新奇
- 生活議題、休閒娛樂
- 社交群體、健康養生

防範方式

- 關閉自動下載圖片
- 關閉預覽視窗
- 設定以純文字格式讀取郵件
- 不要自動回覆讀信回條

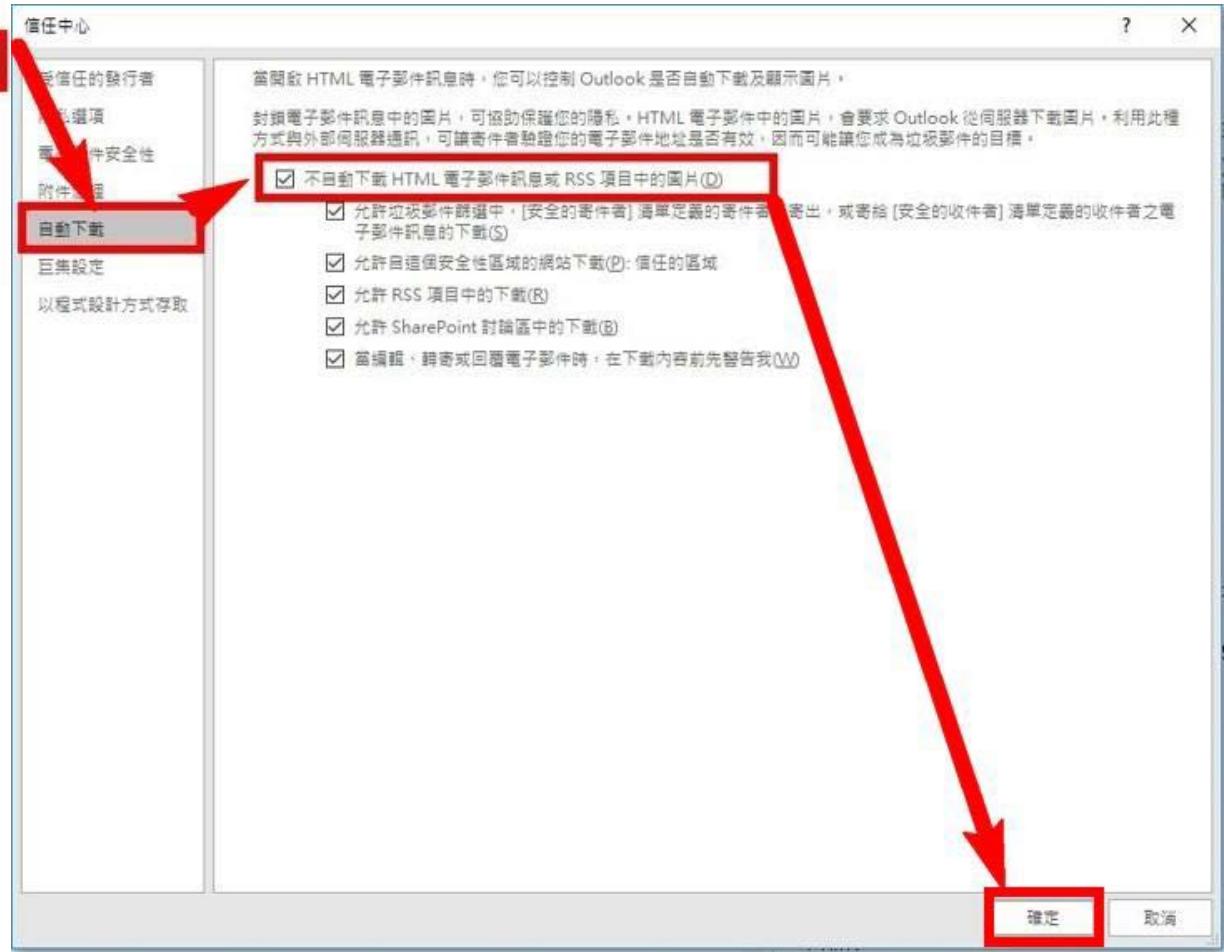
Outlook 2016 安全性設定 關閉預覽視窗

開啟 Microsoft outlook選取 【檢視 】→【讀取窗格 】→【關閉 】

Outlook 2016 安全性設定 關閉自動下載圖片

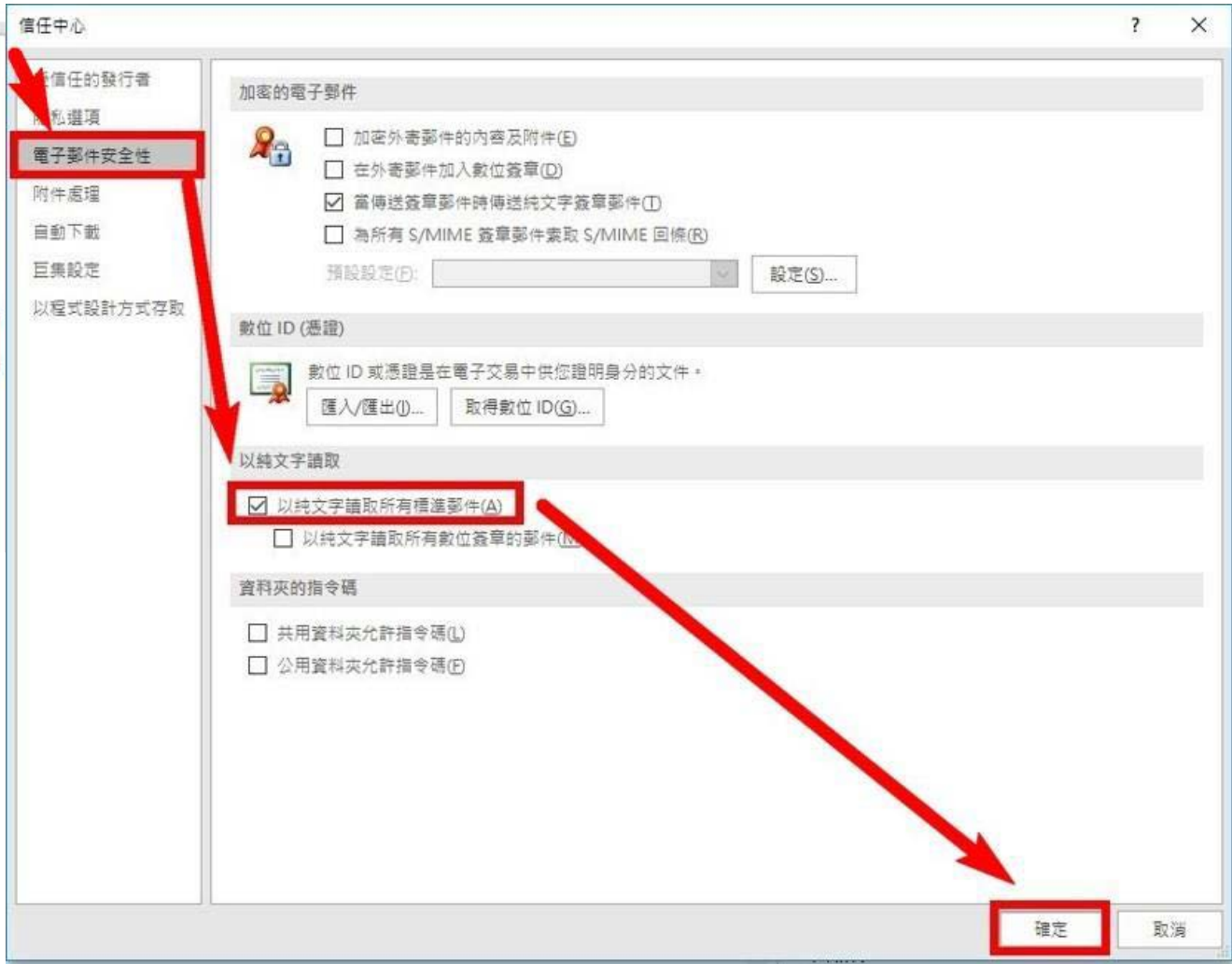
點選 【檔案 】 → 【選項 】 →跳出 【OUTLOOK 選項 】 →【信任中心 】 選項 →【信任中心設定 】→【自動 下載 】→【不自動下載 HTML 電子郵件訊息或 RSS 項目中的圖片 】打勾（預設皆打勾)→【確定 】後變更完畢

Outlook 2016 安全性設定 關閉自動下載圖片



Outlook 2016 安全性設定 以純文字讀取

點選 【檔案 】 → 【選項 】 →跳出 【OUTLOOK 選項 】 →【信任中心 】 選項 → 【信任中心設定 】→【信任中心 】 → 【電子郵件安全性 】 → 【以純文字讀取 】→ 【確定 】後變更完畢 。



判斷電子郵件安全從自己做起

- 關閉自動下載圖片
- 關閉預覽視窗
- 設定純文字格式讀取郵件
- 不要自動回覆讀信回條

- 不開啟來路不明的電子郵件
- 不轉寄不可信任來源之郵件

（以避免擴大受害者）

- 為何我會收到這封郵件
- 我是否應該收到這封郵件
- 我是否應該開啟這封郵件

網路釣魚

- 利用偽造的網頁作為誘餌，詐騙使用者洩漏如帳戶密碼等個人機密資料
- 釣魚網頁畫面與官方網站相同 ，但其實這個網址並非官方網站
- 以相似的字元來偽裝網址， 例如：以數字的0來替換英文的0 以數字的1來替換英文的l
  - 常見的手法有[近似]及[延伸]
  - 近似範例：
    - login.live.com→login-live.com
    - http://www.gamannia.com http://www.gamania.com
    - www.landbank.com.tw www.1andbank.com.tw

駭客會購買關鍵字廣告針對如「網路銀行」、「線上購物」等線上交易網站進行釣魚攻擊，民眾經由搜尋引擎，搜尋到這些關鍵字時，不疑有它，掉入駭客精心設計的陷阱裡。

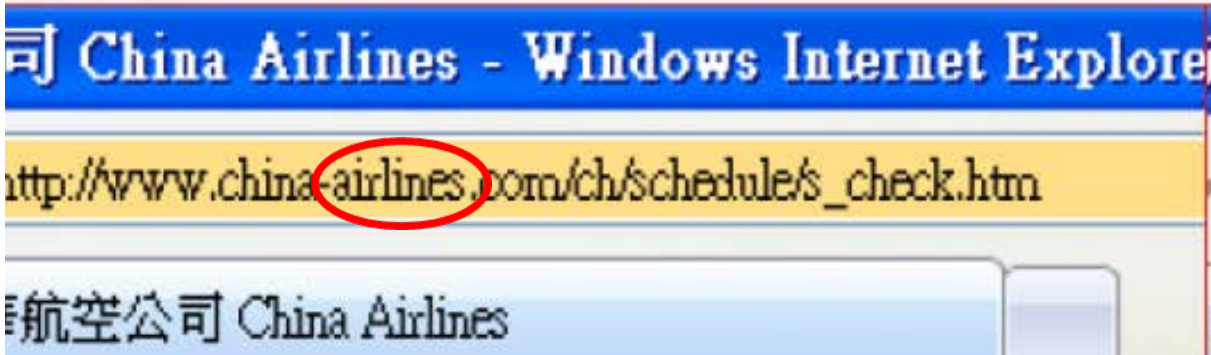
細膩的手法攻擊方式有：

- pchome→pch0me
- International→1ternational
- Myspace → Myspacce
- http://www.landbank.com.tw → http://www.1andbank.com.tw
- m → rn; w → vv ; facebook → faecbook

偽造假冒的網站


http://www.china-airlines.com/ch/schedule/s_check.htm
中華航空公司 China Airlines
CHINA AIRLINES
華夏會員專區
會員卡號
GO
加入會員
密碼查詢
卡號查詢
申請密碼
班機離到動態
網上訂票 | 班表查詢
啓程地區
啓程地點
亞洲
TPE-台北


http://www.china-airlines.com/ch/schedule/s_check.htm
中華航空公司 China Airlines
CHINA AIRLINES
華夏會員專區
會員卡號
GO
加入會員
密碼查詢
卡號查詢
申請密碼
班機離到動態
網上訂票 | 班表查詢
啓程地區
亞洲


China Airlines - Windows Internet Explore
http://www.china-airlines.com/ch/schedule/s_check.htm
航空公司 China Airlines


航空公司 China Airlines - Windows Inter
http://www.china-airlines.com/ch/schedule/s_ch
中華航空公司 China Airlines

八大種類

八大種類

Line免費貼圖詐騙中，請保護好你的Line ID

LINE免費貼圖詐騙（line ID、FB ID、手機號碼...）
http://www.techbang.com/posts/12286

別再相信 Facebook 上的假貨電商

先有幾個認知：

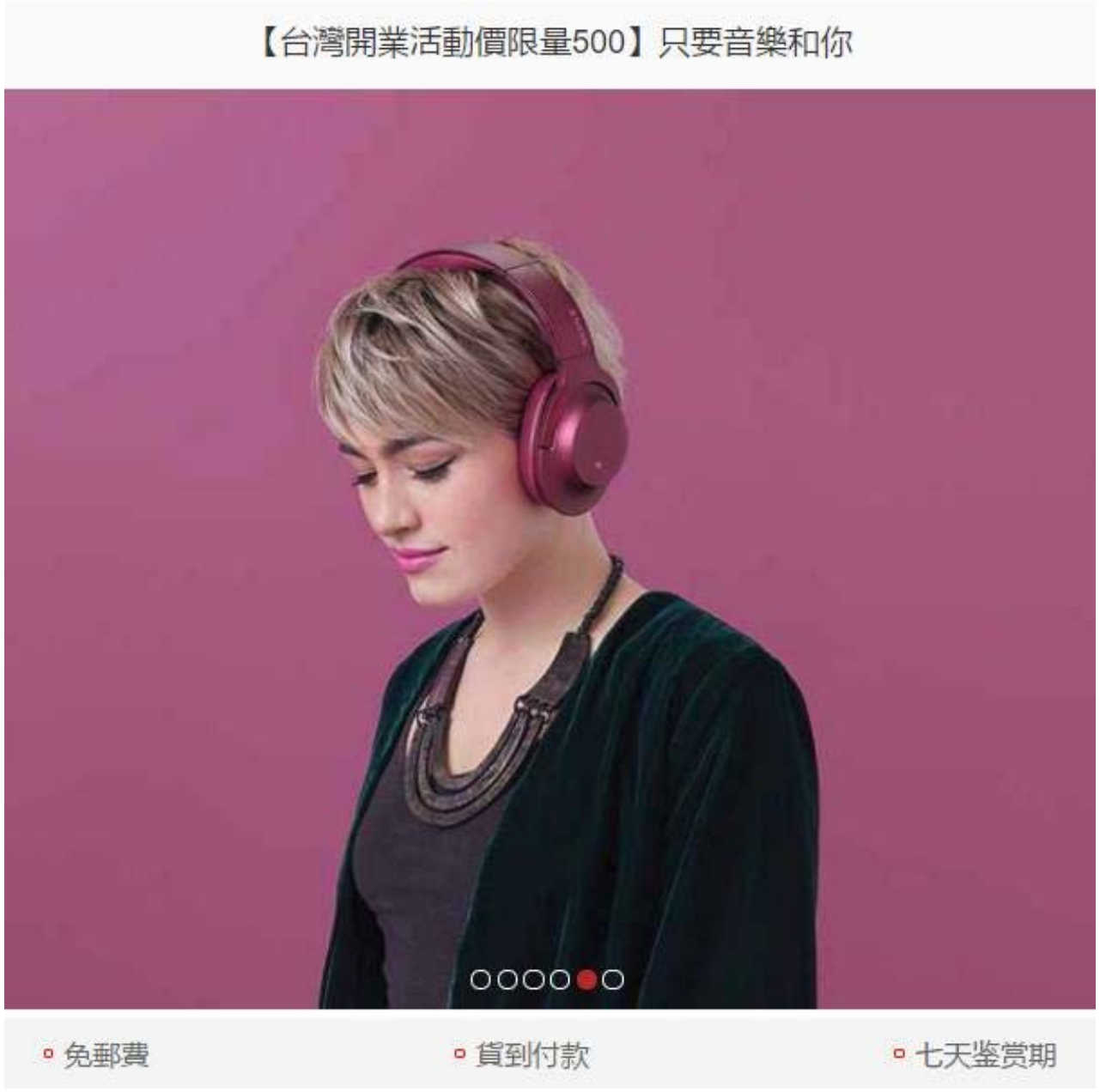
1. 真正知名品牌貨很貴，不管哪一個知名廠牌。
2. 貨到付款的千萬別買。
3. 買到不是中樂透，而是會樂極生悲。

裡面有很多很漂亮的盜用原廠的圖文資料：

詐騙集團利用了兩個人性弱點：
(1)貪小便宜，而且圖文很吸引人
(2)七天鑑賞期，而且貨到付款感覺好安全。(no no no !!)

裡頭還留了「台北店開業祝賀」，地址是「台北舊宗路一段 188 號 1 樓」，別高興，那是大潤發，並非詐騙業者的「台北店」。

https://www.inside.com.tw/2017/05/07/facebook-fraud



- Facebook惡意程式病毒，會假冒你的名義擴散，還會安裝來路不明的外掛程式

https://www.kocpc.com.tw/archives/11060

- Facebook「假功能/假驗證、真盜資料」詐騙

https://www.kocpc.com.tw/archives/6178

Q & A