

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料司。
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

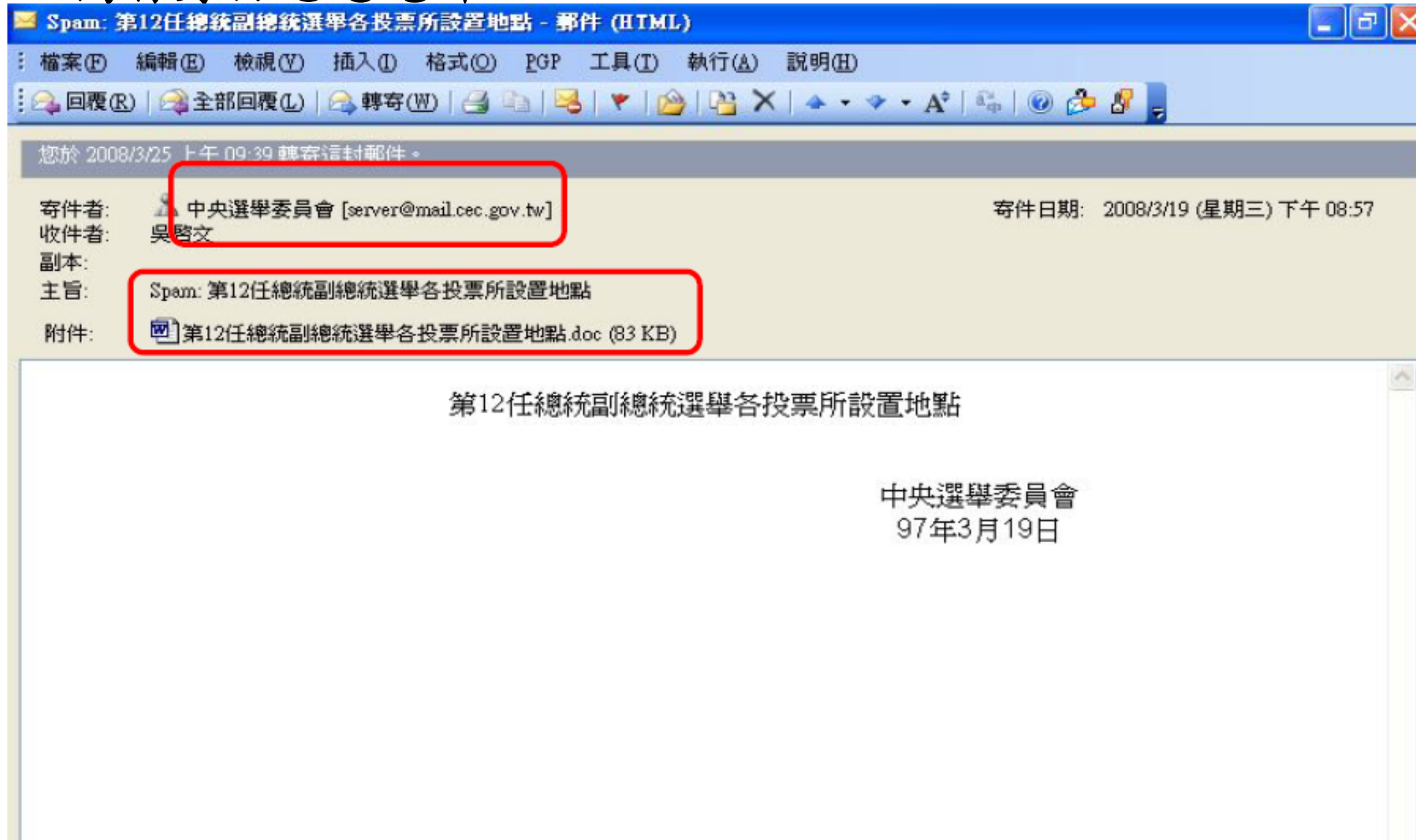
電子郵件攻擊手法

混淆視聽之郵件寄件者

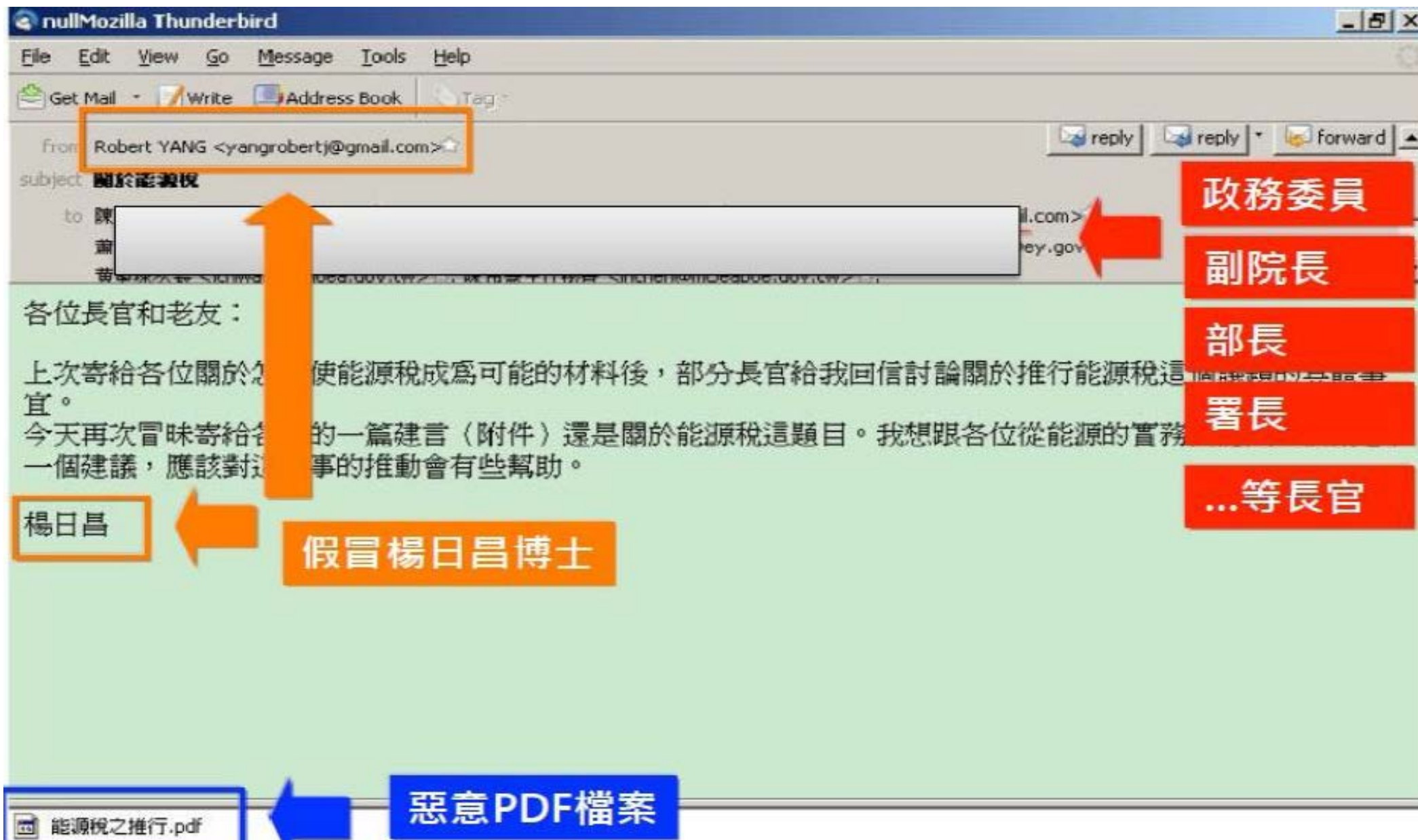
- 偽裝身分(王小明、Alex)
- 偽裝機關(AB銀行、XY商店)
- 偽裝服務(OX論壇電子報、YAHOO新聞)
- 附件夾帶病毒~蠕蟲~木馬程式及殭屍程式等惡意程式
- 郵件本文夾帶惡意連結
- 假冒使用者信任的人，讓使用者相信電子郵件的內容，而去開啟附件或超連結，暗中啟動木馬程式

電子郵件攻擊手法

□ 偽冒身份惡意電郵



偽冒身份惡意電郵



□含有惡意程式的附件-偽裝報稅通知訊息

From: 財政部電子申報繳稅服務 [mailto:server@tax.nat.gov.tw]
Sent: Thursday, April 28, 2011 9:05 AM
To: linda_w@lil.org.tw
Subject: 綜合所得稅電子結算申報繳稅100年5月1日開始開始了！

Dear Dr. Ke:
FYI,
Best,
Linda

電子申報

注意(公告)事項
個人綜合所得稅電子結算申報繳稅系統申報日期為100年5月1日起至5月31日

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IRX12.00版 更新日期: 100-4-14

綜合所得稅電子結算申報繳稅106年5月1日開始了
附加檔案：使用說明.DOC

TheDocument.doc - Microsoft Word

綜合所得稅電子結算申報繳稅使用說明

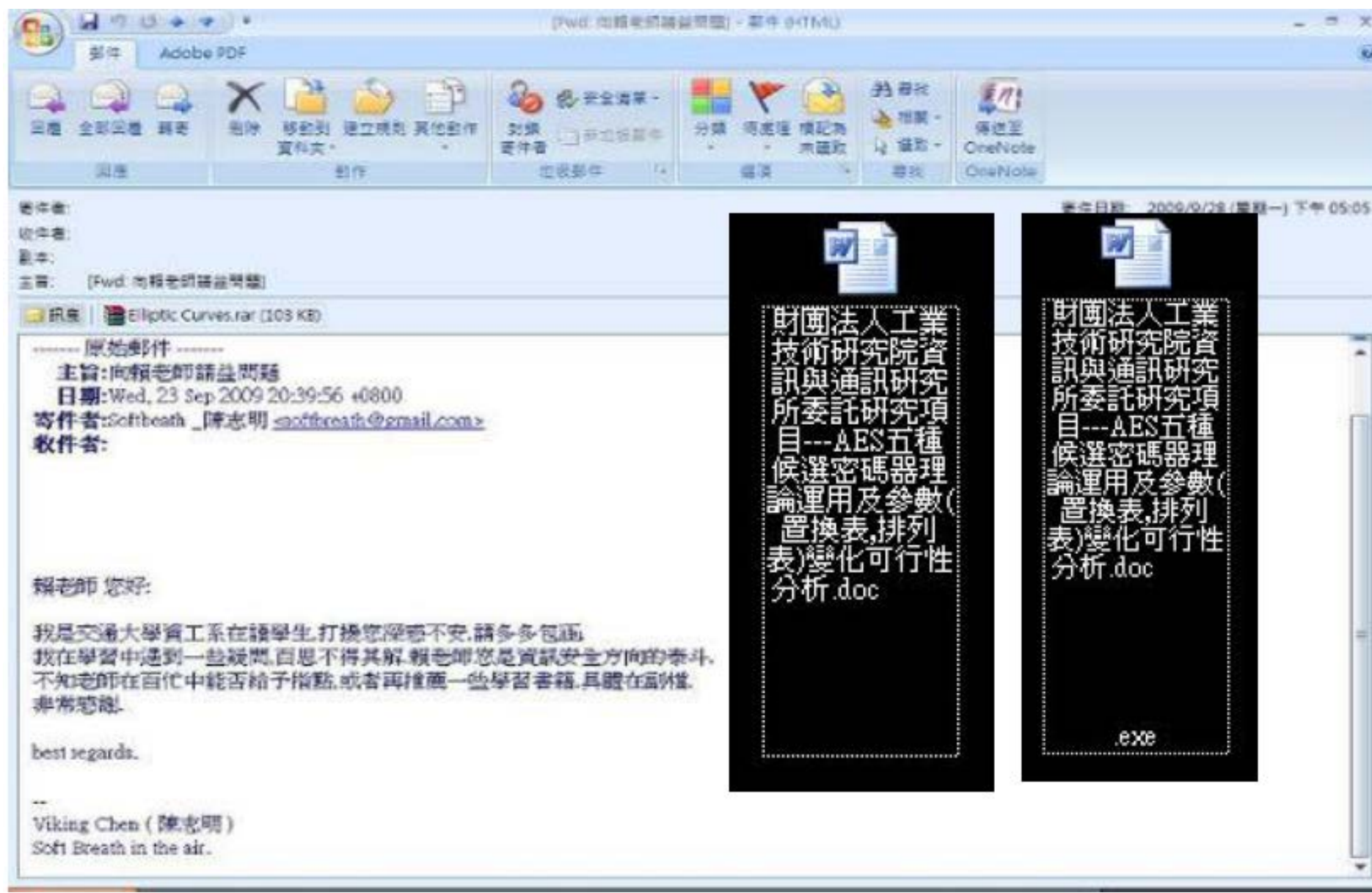
查詢99年度所得及扣除額資料說明

- 欲查詢當年度所得及扣除額資料者，必須使用憑證(自然人憑證 IC 卡、硬金證憑證)，下載安裝本系統，以上述任一憑證登入申報系統後，才能進行下載、查詢作業。
- 若您於100年3月1日至3月15日，有申請所得資料下載(於本網站或補稅機關申請)，且申請成功者，其下載所得會受申請類別影響：分戶資料限制下載--您使用申報系統下載所得後，僅能看到您自己所得資料，無法看到配偶及未成年子女之所得及扣除額資料。
- 欲申請憑證者，請參閱「憑證申請」網頁；申報系統軟體下載，請點「軟體下載」網頁。

綜合所得稅電子結算申報繳稅系統-使用說明教學

- 教學檔使用說明：下載完成後請先進行解壓縮，完成解壓縮後執行目錄下之.html檔(如：綜合所得稅電子結算申報繳稅申報教學說明.html)。
- 綜合所得稅網路申報作業教學檔
- http://download.tax.nat.gov.tw/irs/TRX.zip
- 綜合所得稅二維申報作業教學檔

□ 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

The image shows the Outlook 2016 settings interface. A red arrow points from the top-left corner to the 'Trust Center' option in the left-hand navigation pane. Another red arrow points from 'Trust Center' to the 'Trust Center Settings' button. A third red arrow points from 'Trust Center Settings' to the 'Automatic Download' option in the left-hand navigation pane of the Trust Center dialog. A fourth red arrow points from 'Automatic Download' to the checkbox 'Do not automatically download HTML images or RSS items in this message' (不自動下載 HTML 電子郵件訊息或 RSS 項目中的圖片), which is checked. A final red arrow points from this checkbox to the 'OK' button at the bottom right of the dialog.

Outlook 選項

一般
郵件
行事曆
人員
工作
搜尋
語言
進階
自訂功能區
快速存取工具列
增強性
信任中心

協助您維護文件的完整性，並讓您的電腦維持在安全且良好的狀態。

安全性和其他

造訪 Office.com 以瞭解更多關於保護您的隱私權和完整性的資訊。

[Microsoft 可信度連線圖標](#)

Microsoft Outlook 信任中心

信任中心包含對安全性和隱私權設定，這些設定將協助您保護您的文件，並防止您的電腦被惡意軟體感染。

信任中心設定

信任中心

當開啟 HTML 電子郵件訊息時，您可以控制 Outlook 是否自動下載及顯示圖片。

對類電子郵件訊息中的圖片，可協助保護您的隱私。HTML 電子郵件中的圖片，會要求 Outlook 從伺服器下載圖片，利用此種方式與外部伺服器通訊，可讓寄件者驗證您的電子郵件地址是否有效，因而可能讓您成為垃圾郵件的目標。

不自動下載 HTML 電子郵件訊息或 RSS 項目中的圖片

允許您在郵件群組中，[安全的郵件寄] 清單定義的郵件寄件者，或寄給 [安全的收件者] 清單定義的收件者之電子郵件訊息的下載

允許自這個安全性區域的網站下載 (D): 信任的區域

允許 RSS 項目中的下載 (R)

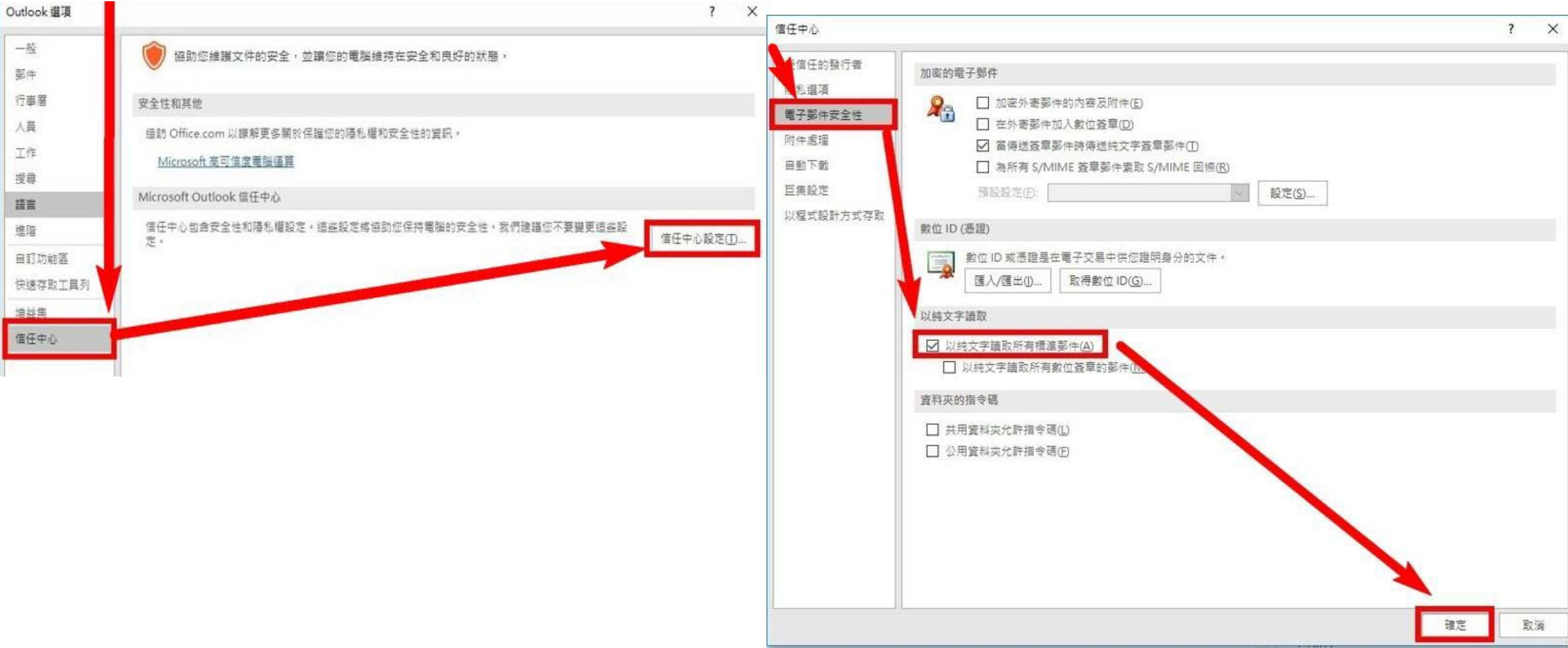
允許 SharePoint 討論區中的下載 (B)

當編譯、轉寄或回覆電子郵件時，在下載內容前先警告我 (W)

確定 取消

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

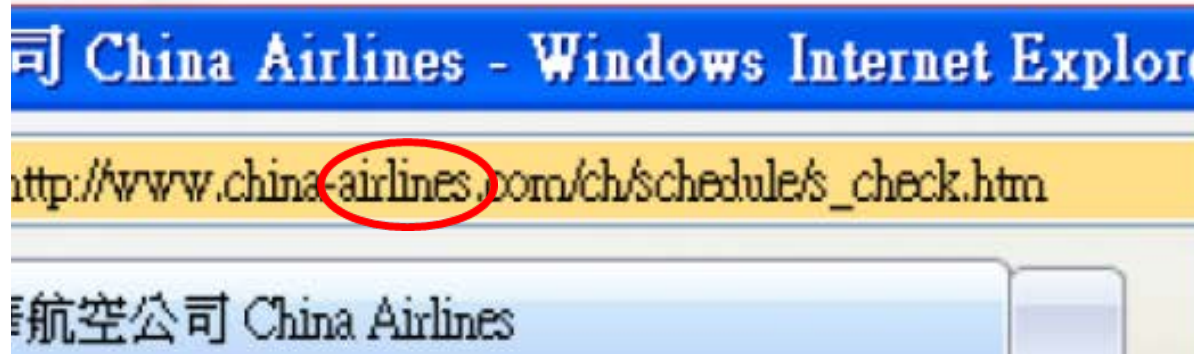
- ▣ 利用偽造的網頁作為誘餌，詐騙使用者洩漏如帳戶密碼等個人機密資料
- ▣ 釣魚網頁畫面與官方網站相同，但其實這個網址並非官方網站
- ▣ 以相似的字元來偽裝網址，例如：以數字的0來替換英文的O 以數字的1來替換英文的l
- ▣ 常見的手法有[近似]及[延伸]
- ▣ 近似範例：
 - ▣ login.live.com→login-live.com
 - ▣ http://www.gamannia.com http://www.gamania.com
 - ▣ www.landbank.com.tw www.1andbank.com.tw

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：

- pchrome → 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



八大種類



免費送 巧連誌影音教材
家有10歲以下小朋友的家長，快來免費體驗巧連誌影音教材
國小以下：送生動有趣VCD；小一以上：送精美學習碟
還有機會抽中巧虎食物派對組囉

免費送

購物



茂德增貸「打六折」通過 銀行團提供30億元

DRAM大廠茂德的增貸案，今(16)日晚間又有最新進展，八家行庫經過長達的十小時的討論後，最後同意增貸案過關。不過金額只有30億元，與茂德原本提出的50億元，仍有一段差距，而這份最後得由茂德再另想辦法。



金融



你覺得民代可以基於何政理由，蒐集使用民不個人資料嗎？

有立委擬提案增列「民代免責條款」，基於同政理由蒐集個人資料時，用告知當事人，引起了正反兩方意見的論辯。

立委提案增打個資法立委免責條款，讓立委問政可不經告知而任意蒐集債、政黨傾向、升遷等個人資料，並獲法務部同意，民間司改會律師洪說，若立法院通過法案，有可能讓立法院成為全國最大的徵信社，並助長化；也有檢察官說，這有違法務部宣傳海報「個資無國界，保護零成象號。法務部面對各界撻伐，昨晚突一改立場表示「還憂審慎評估」。



政治

(詳全文)



殺Online線上遊戲桌布



遊戲

八大種類



風光收入
當紅時髦一展睇呀的100萬
一天賺兩萬
每月收入可達10萬
可賺100萬

八卦

(詳全文)

資深藝人...
出錢贊助...
藝人高凌...
趣、高凌...
以幫忙解...
人，最主...



其只有1.5倍。』

邱琬婷指出，一般民眾防曬只記得短波的UVB，預防曬紅、曬傷，卻容易忽視長波UVA的照射，她說，UVB其實只佔所有紫外光的5%而已，但曝曬UVA容易導致皮膚敏感，皮膚耐受力變差，色素形成，皮膚老化，色素沈澱，甚至誘發皮膚癌。邱醫師呼籲，民眾平時，挑選具有PA或PPD指數以及SPF的產品，全方位防護以預

無法抗拒的
誘惑天使美唇
\$199
調查：座位票當選 46%

醫藥



32 女人誌
31 男人誌

蛋糕房
金焱俏女郎
溫泉
女我

情色



2009台北國際花卉展開幕典禮

娛樂

2009台北國際花卉展開幕典禮!

2009臺北花卉展在台北小巨蛋舉行，3月11日至3月15日共展出七大佈景，包括主題印象區、新品種展示區、花博意象區、蘭花競賽區、國內外企業區等，以花彩繪人生、以綠活絡社區和保護地球環境為三大設計方針，主題放在「花之舞」，希望藉由花卉組裝的容顏來「舞動」花博，為花博暖身。

主題印象區以世界之名舞蹈，帶出各種不同以花形塑的花之舞者，像是藍調舞斗的「彩花悠路」，用輕柔動人的洋娃娃和各種可愛的蕊蕊，搭配閃閃亮亮的

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>

【台灣開業活動價限量500】只要音樂和你



免郵費

貨到付款

七天鑑賞期

□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