資訊安全與社交工程

大綱

- 熱門詐騙及攻擊手法分享
- 何謂社交工程
- 惡意電子郵件類型介紹
- 網頁連線資訊收集演示
- 辨別危險網址與詐騙
- 使用者如何提升防範意識
  - *電子郵件使用安全認知*
  - *密碼安全性設置*
  - *收件軟體安全設置說明*
- 正確郵件危機意識與觀念

為什麼資訊安全如此重要?

- 公司業務停擺、名譽受損、失去客戶
- 造成公司巨額金錢損失、罰款
- 重要檔案遺失或被加密
- 相關人員連帶受罰
- 失去工作、負擔損失、官司纏身

熱門詐騙及攻擊手法分享

資安事件回顧

- 不停止的惡意郵件
- 勒索病毒的發展
- 假新聞攻擊事件影響整個網路安全
- 家庭網路威脅升溫
- AI潛藏的道德風險與資安危機

網路現今的環境

- **惡意郵件與網址釣魚**

網路釣魚一直是駭客最常使用的郵件攻擊手法，因為這種方式最簡單有效。

釣魚攻擊可分為好幾種類型，最常見的就是假冒登入頁面。駭客會先利用合法的網頁空間架設釣魚網站，接著使用電子郵件寄送帳號異常通知信，要求您必須盡快登入，確認帳號是否正常運作。當您點擊連結時，會跳轉到一個與該系統服務極為相似的釣魚網站，誘騙受害者輸入指定資訊後，藉此盜取帳號密碼或信用卡等機敏資料。

勒索軟體 (Ransomware)

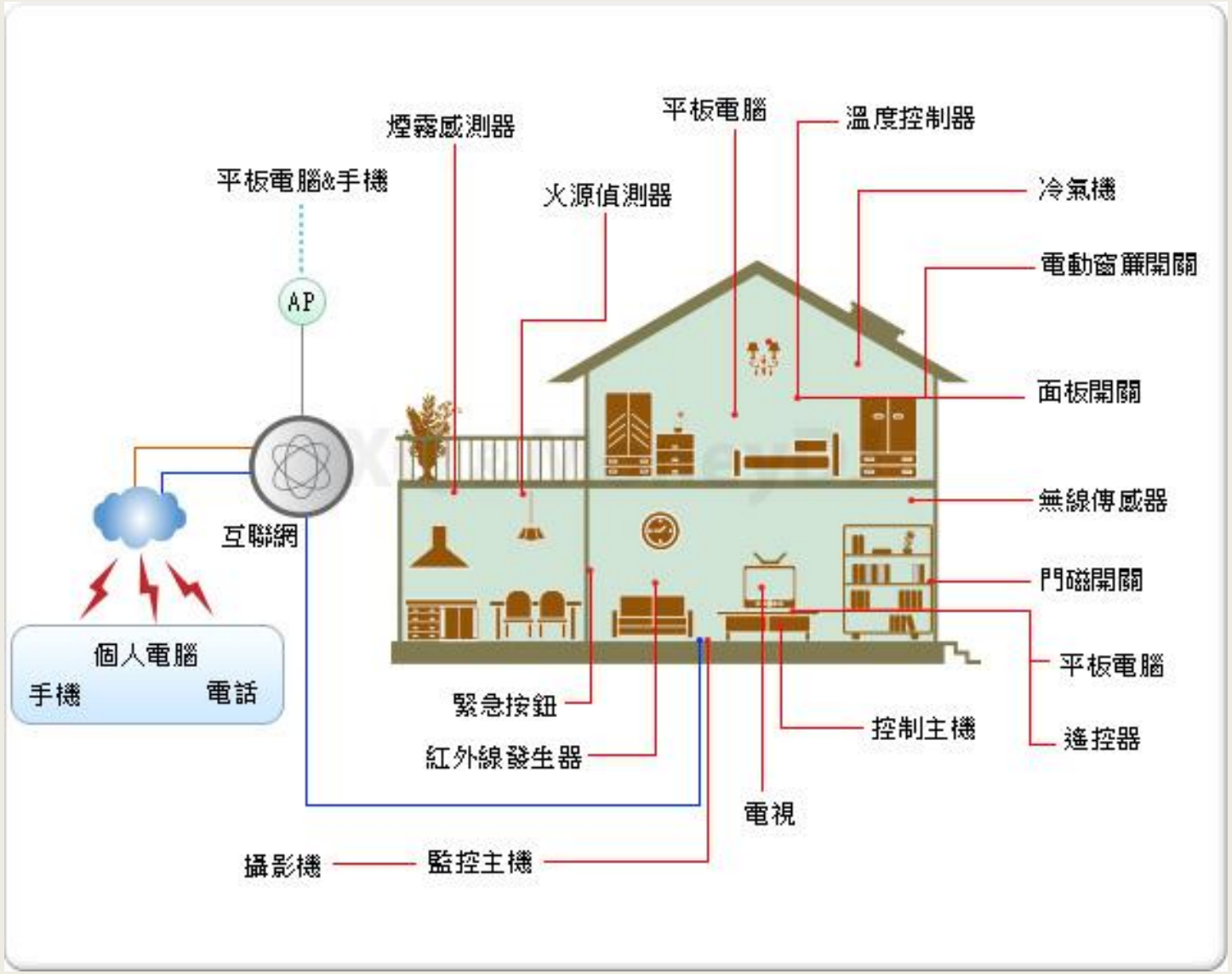
- **破壞對象**：電腦內Word（doc、docx）、Excel（xls、xlsx）、PowerPoint（ppt、pptx）、JPG圖檔等近百種企業常見檔案格式。
- 攻擊方式：向遠端遙控主機取得加密金鑰，再以2,048位元RSA和AES加密技術
- 攻擊範圍：受害電腦連結的網路芳鄰、網路磁碟機、檔案伺服器等，攻擊公司內網所有共享的文件（New卸除式裝置）
- 限制期限內匯款（信用卡、ATM、彼特幣）
- 即使發現刪除惡意軟體，文件也無法救回

假新聞攻擊事件

境外資訊戰手法不斷翻新，假新聞威脅不容忽視

作者 侯 冠州 | 發布日期 2021 年 09 月 30 日 10:44 | 分類 社群 , 科技生活 , 網路

家用智能產品與網路


煙霧感測器
平板電腦
溫度控制器
平板電腦&手機
火源偵測器
冷氣機
電動窗簾開關
AP
面板開關
無線傳感器
互聯網
門磁開關
個人電腦
手機
電話
平板電腦
遙控器
緊急按鈕
控制主機
紅外線發生器
電視
攝影機
監控主機

智慧產品風險事件

避免網路攝影機被入侵遭偷窺

生成式AI潛藏的道德風險與資安危機

辨別詐騙網址

網址範例

- 偽造案例：

中國信託
- www.chiinatrust.com.tw
- www.chinatrust.com.tw

花旗銀行
- www.citibahk.com
- www.citibank.com

匯豐銀行
- www.hshc.com.tw
- www.hsbc.com.tw

財政部北區國稅局
- www.ntx.gov.tw
- www.ntx.com.tw

雅虎拍賣
- TW.BID.YAHOO.COM
- TW.BlD.YAHO0.COM

無名小站
- www.vvretch.cc
- www.wretch.cc

網路家庭
- www.pchome.com.tw
- www.pchorne.com.tw

新光人壽
- www.skl.com.tw
- www.sk1.com.tw

1111人力銀行
- www.1111.com.tw
- www.11111.com.tw

可以注意的地方

以下是一些方法可以幫助你辨別詐騙網址或偽造網址：

- 檢查網址的拼寫和格式：詐騙網址通常會修改正確的拼寫或稍作變化。仔細檢查網址的拼寫和格式，確保它與正確的網址相符。
- 注意網址的域名：觀察網址的域名部分（例如www.example.com），詐騙者可能使用類似但稍有不同的域名，例如更改.com為.net，或添加額外的單詞。
- 使用安全連接（HTTPS）：詐騙網站通常不使用安全的HTTPS連接。在瀏覽網站時，確保網址開頭為"https://"而不是"http://"，並且在瀏覽器中顯示有一個鎖形圖示。

QR CODE連線資訊收集演示

QR CODE掃描小測試

http://www.wken.tw/sce_link/sce_list.php?k=2021

瀏灠網頁可收集到的資訊

- 可收集到的資訊：
  1. *確認郵件是存在的*
  2. *連結本身帶的資訊 (www.abc.com.tw/abc/168/)*
  3. *IP*
  4. *瀏灠器及版本*
  5. *作業系統、位元數及版本*
  6. *設備廠牌、型態*
  7. *其他(語系、地區、電信商)*

- 以上僅是資訊收集，還不包含網站本身的陷阱

社交工程說明

社交工程是?

•社交工程是利用人性弱點進行詐騙，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。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。

•社交工程有兩個基本原件：
- 第一個是【詐騙的對象】
- 第二個是【詐騙的手法】

•凡對【目標】甚至是【特定的對象】，使用各種新奇古怪、八股或創新的【詐騙手法】，來達到施騙者的目的。

社交工程的攻擊原因

- 無論再堅強的陣容及防護設備，只要存在【人】這因素，就一定有【漏洞】存在
- 駭客利用漏洞百出的【人性】，來設計各式各樣的【詐騙手法】

- 貪心：撿便宜的個性
- 情色：食色性也多多益善
- 好奇：探索八卦訊息的個性
- 驚恐：威脅恐嚇讓人慌亂
- 信任：輕易的相信不求實證
- 不在意：沒那麼倒楣吧的想法
- 警覺力：無所謂後果的嚴重性

社交工程手法不只一種?

- 網路釣魚主要也仰賴的是社交工程技巧，那麼很重要的一點就是，所有使用者都應了解駭客如何利用人性的弱點。
- 社交工程技巧是一種駭客用來說服使用者做某些動作的騙術，使用者在平常的時候通常不會做這些事。
- 社交工程技巧有時很單純，例如現實生活中的協尋遺失物

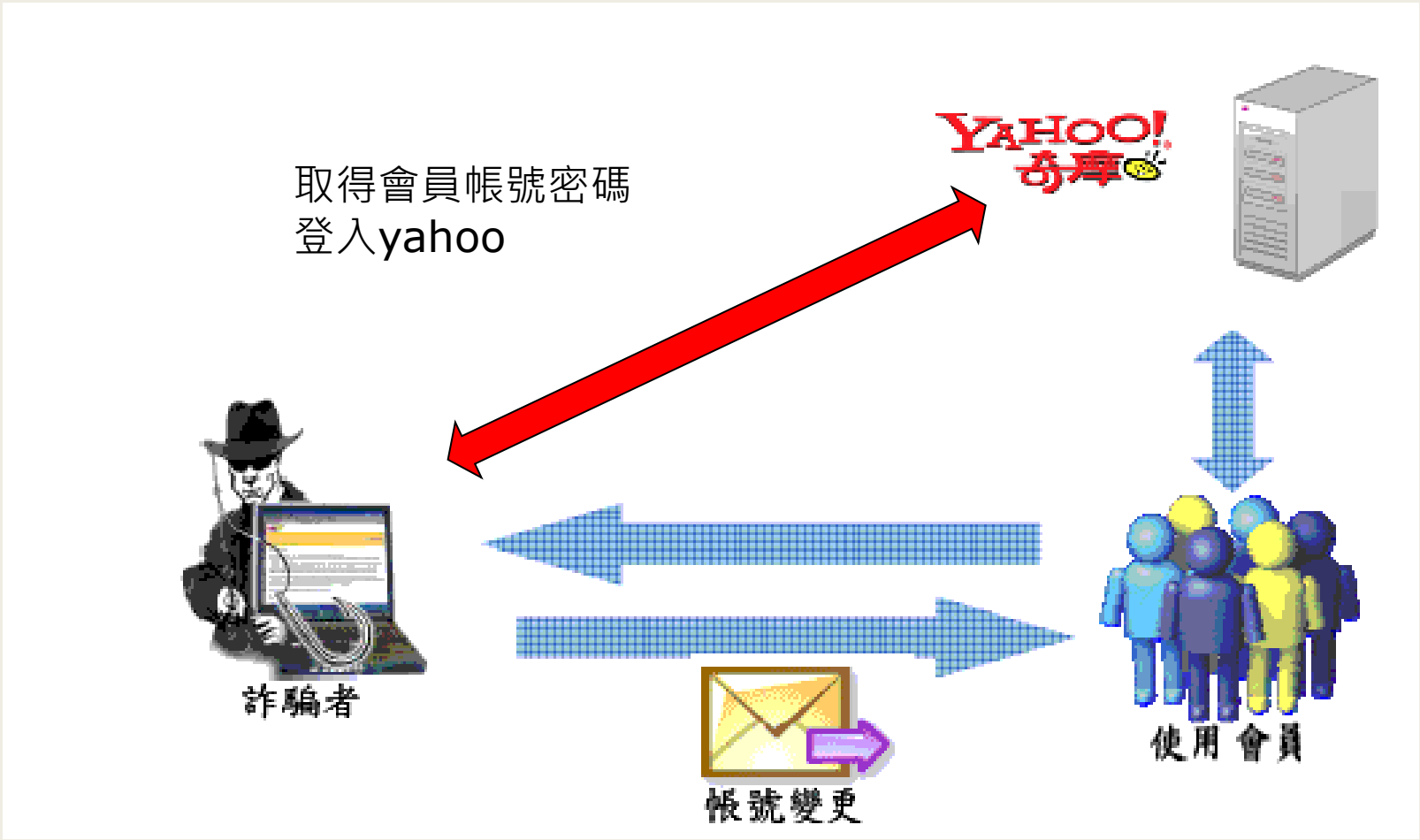
最常見的攻擊

- **社交工程的攻擊行為**

- **駭客透過最常使用-收發電子郵件來進行攻擊，使用的方法是發送電子郵件給握有機密資料的使用者。**

- **社交工程信件請收件人員確認附件檔案裡所提到的問題，或在加入連結網址於郵件本身，進而讓使用者開啟附件或點擊連結，以便植入並啟動木馬程式**

社交工程攻擊例子-1



電子郵件社交工程郵件?

電子郵件社交工程：

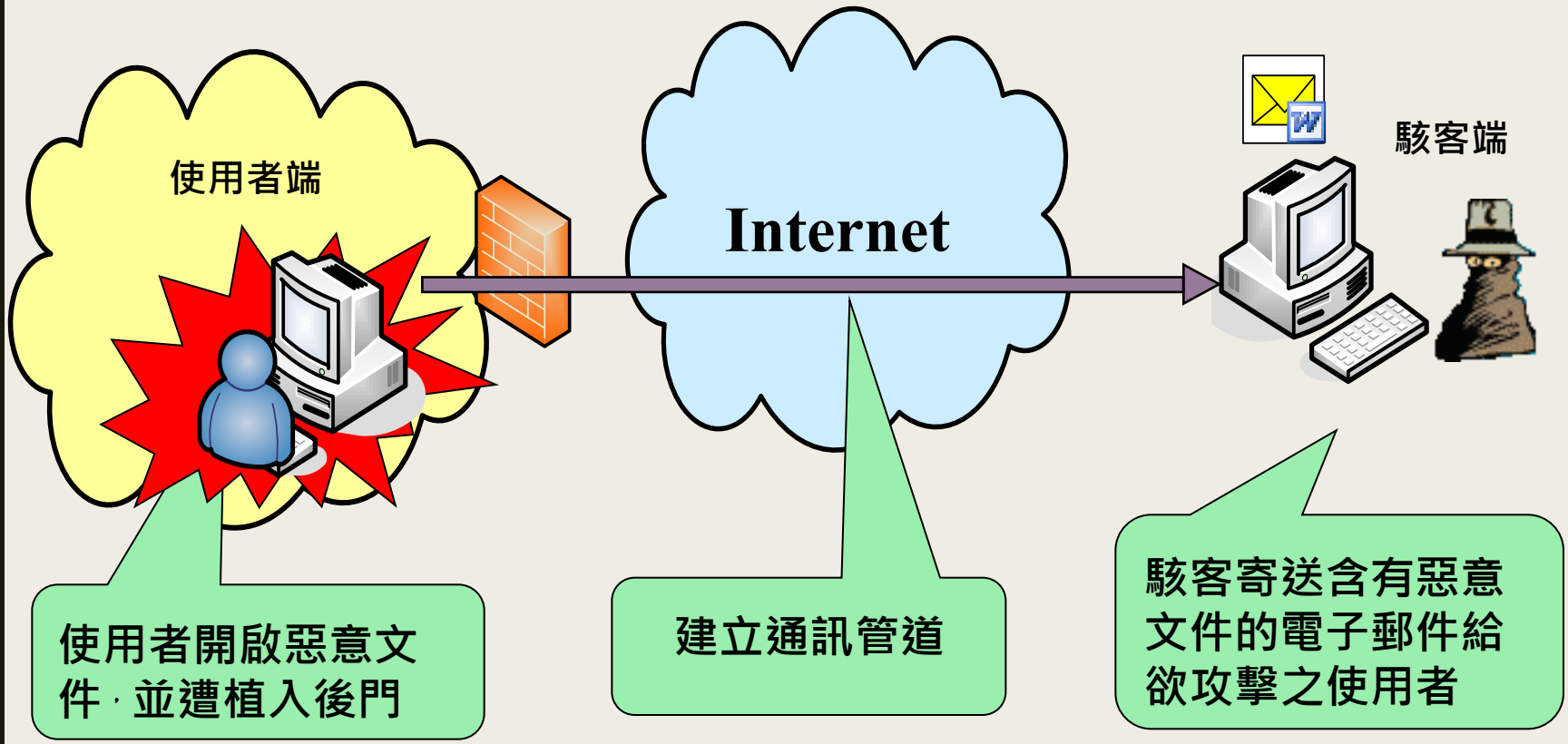
- **藉由傳送電子郵件方式，騙取收件者信任，進而開啟郵件內容的駭客攻擊模式。**

•透過電子郵件可以讓收件者

- **(1)誘騙進入假網站**
- **(2)開啟惡意電子檔**
- **(3)下載問題檔案**

電子郵件社交工程攻擊模式

利用電子郵件攻擊



電子郵件社交工程攻擊模式

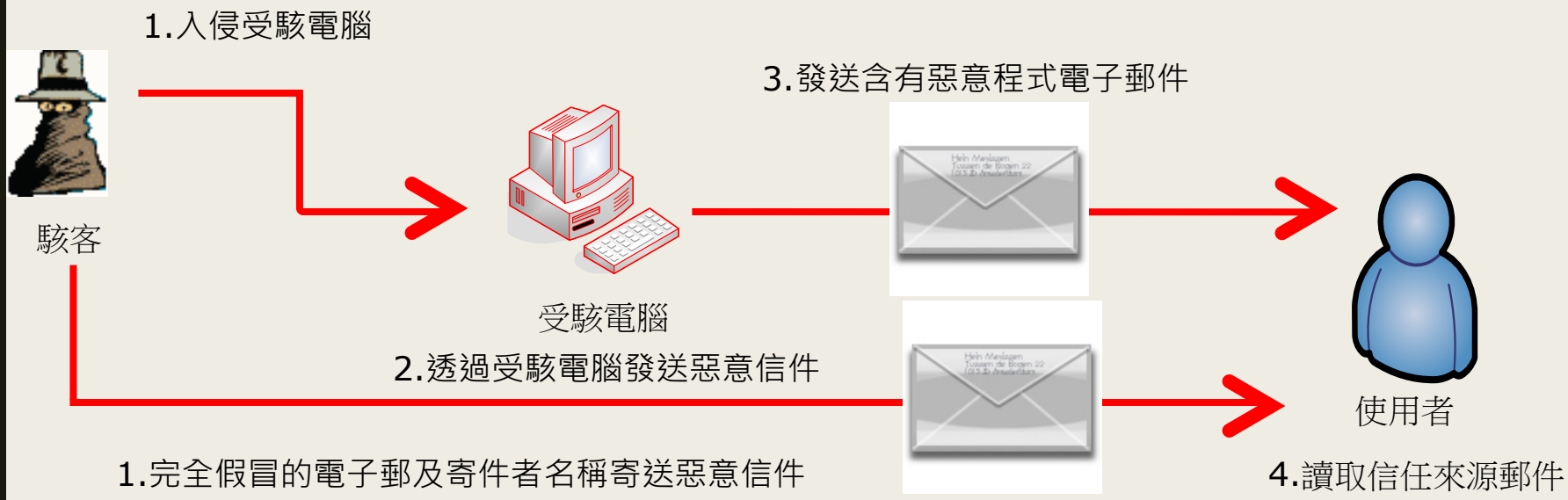
- 假冒寄件者
- 使用讓人感興趣的主旨與內文
- 帶有惡意程式的附件檔案
- 利用零時差(0-Day) 攻擊

假冒寄件者方式-假冒攻擊

- SMTP 通信規範, 沒有辦法限制驗證寄件人的身份. 雖然可以用身份驗證機制確保信是由特定人員寄出(例如加上簽章), 但沒辦法防止別人偽造你的 EMAIL 寄出信件. 頂多只能分辨出信是否為假的...
- 寄件人名稱可以是假的
- 超連結的狀態列可以是假的
- 整封信件，都是假的!!!!!!!!!

假冒寄件者方式 - 完全假冒

- 由於電子郵件傳送協定弱點，駭客可完全假冒寄件者的名稱以及電子郵件位址，甚至可透過入侵寄件者的電腦來寄發電子郵件。



社交工程攻擊例子-2


HiNet網頁郵件服務
HiNet務問題 <
@ms59.hinet.net>
收件者
回覆
全部回覆
轉寄
2020/11/16 (週一) 上午 06:15
通過 SPF 驗證，確認是從 HiNet 服務寄出的信
HiNet
親愛 HiNet，
宣稱電子郵件即將到期，會影響收發信
您的電子郵件 已過期，您可能會遇到電子郵 件傳遞問題.我們建
議您在 24 小時內更新電子郵件，以避免電子郵件發送和接收問題。
安裝電腦防毒軟體、更新病毒碼並完成掃毒。
HiNet WebMail
點擊連結後，會跳轉到釣魚網站
服務 通知信，請勿直接 回覆，謝謝。
祝您 身體健康 萬事如意
中華電信數據通信分公司 敬上
客服專線： 0800-080-411
info@ms1.hinet.net

惡意的電子郵件

使用讓人感興趣的主旨與內文

- 駭客會使用收信者有興趣的八卦、熱門消息、活動消息、情色或工作等相關議題的主旨，來吸引收信者，開啟這些**附件**或**超連結**，植入木馬程式。例如：
  - 旅遊：解封預備 準備好出國
  - 科技：不再是單純金光黨騙局! 六種企業網路釣魚手法再進化
  - 資訊：[提醒] : 您的自動付款詳情
  - 通知：密碼已經更改。

含有惡意程式附件

- 駭客在電子郵件附加含有惡意程式的檔案，這個檔案不一定是執行檔，可能是各種類型的應用程式，甚至是FLASH檔案。

- 駭客可夾帶任何存在作業系統中有弱點文件檔案類型，並誘騙使用者開啟附件檔案，以植入安裝木馬程式。例如：
  - *影片檔（*.wmv）*
  - *Office文件（ *. doc、 *. xls、 *. ppt ）*
  - *圖檔（ *. jpg）*
  - *壓縮檔（ *. zip）*
  - *PDF檔（ *. pdf）*

附件檔案夾帶程式-1


RE: Enquiry (Payment) 查詢（付款）
Yoyo (uangyaoyaozw@126.com) 新增連絡人
2019/9/9 下午 02:15
收件者: c .com.tw;
EnquiryPaym
ent.zip
請小心所有 E-MAIL 中的壓縮檔附件
Dear Sir/Madam,
Thank you for email
Please see Attachemeent of Payment Products
I glad to offer you with a quotation.
Thank you very much!
尊敬的先生/女士，
謝謝你的電子郵件
請參閱付款產品的附件
我很高興為您提供報價。
非常感謝你！
Yoyo as Sales Executive
Skype ozw@126.com
Mobil 3453(Wechat)
Tel:+8 33-642
Keyte chnologies(HK) Limited
www.

附件檔案夾帶程式-2

Undelivered Mail Returned to Sender

Google (composit@cucinecomposit.it) Add contact 8/28/2015 1:53 PM

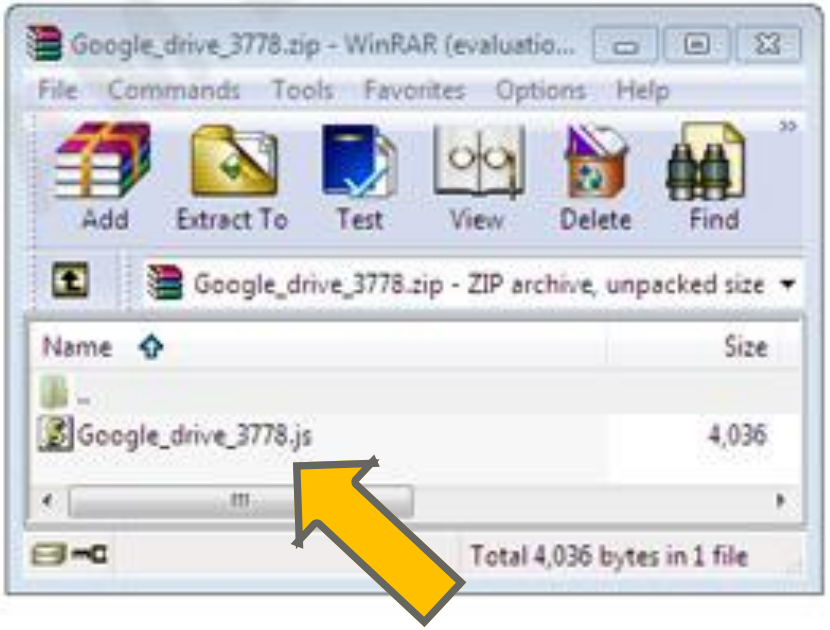
To:

Google_drive_3778.zip

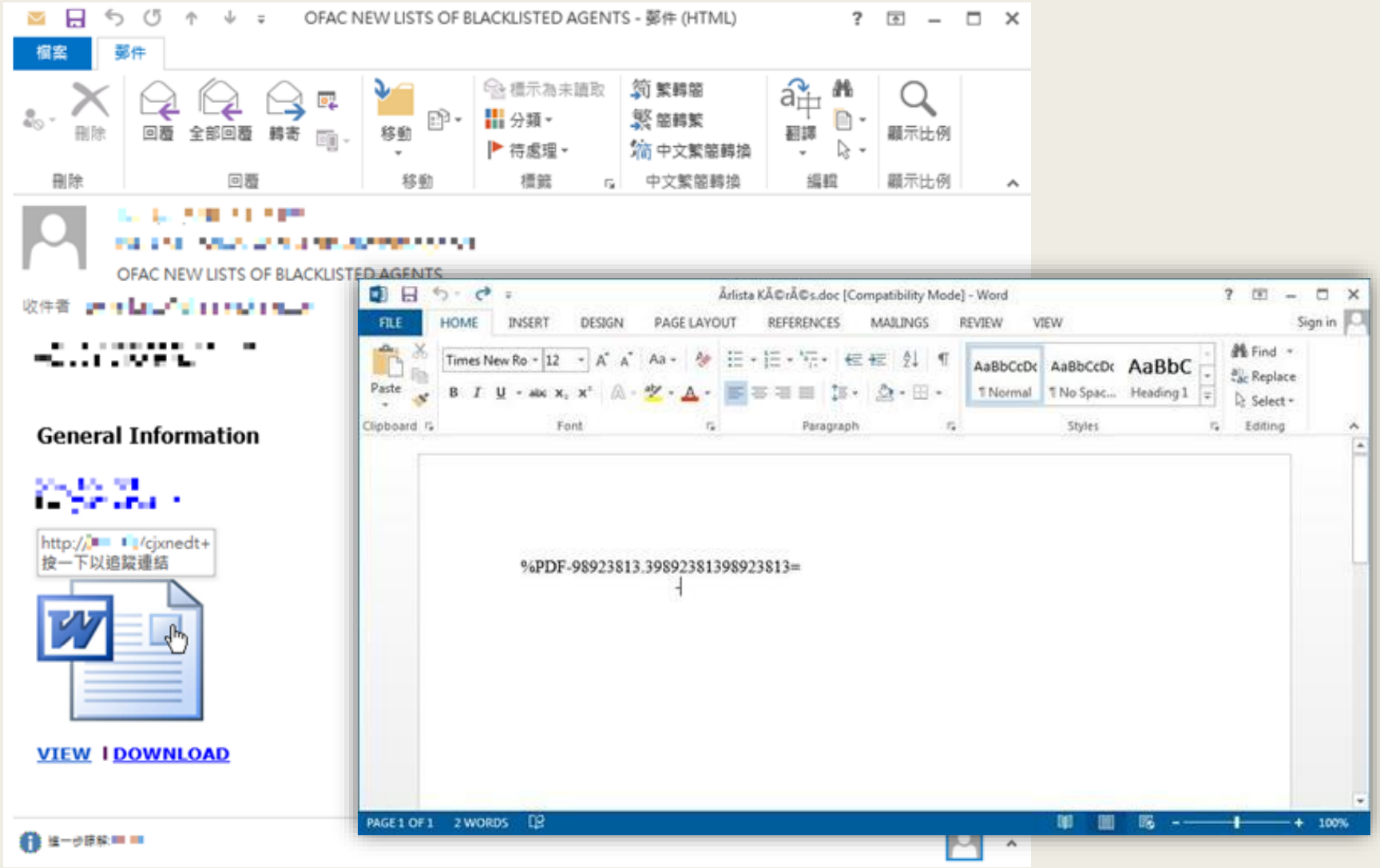
This is the mail system at host mx.google.com.
I'm sorry to have to inform you that your message could not be delivered to one or more recipients. It's attached below.
For further assistance, please send mail to postmaster.
If you do so, please include this problem report. You can delete your own text from the attached returned message.

The mail system

Host or domain name not found. Name service error for name=a-google.com type=A: Host not found



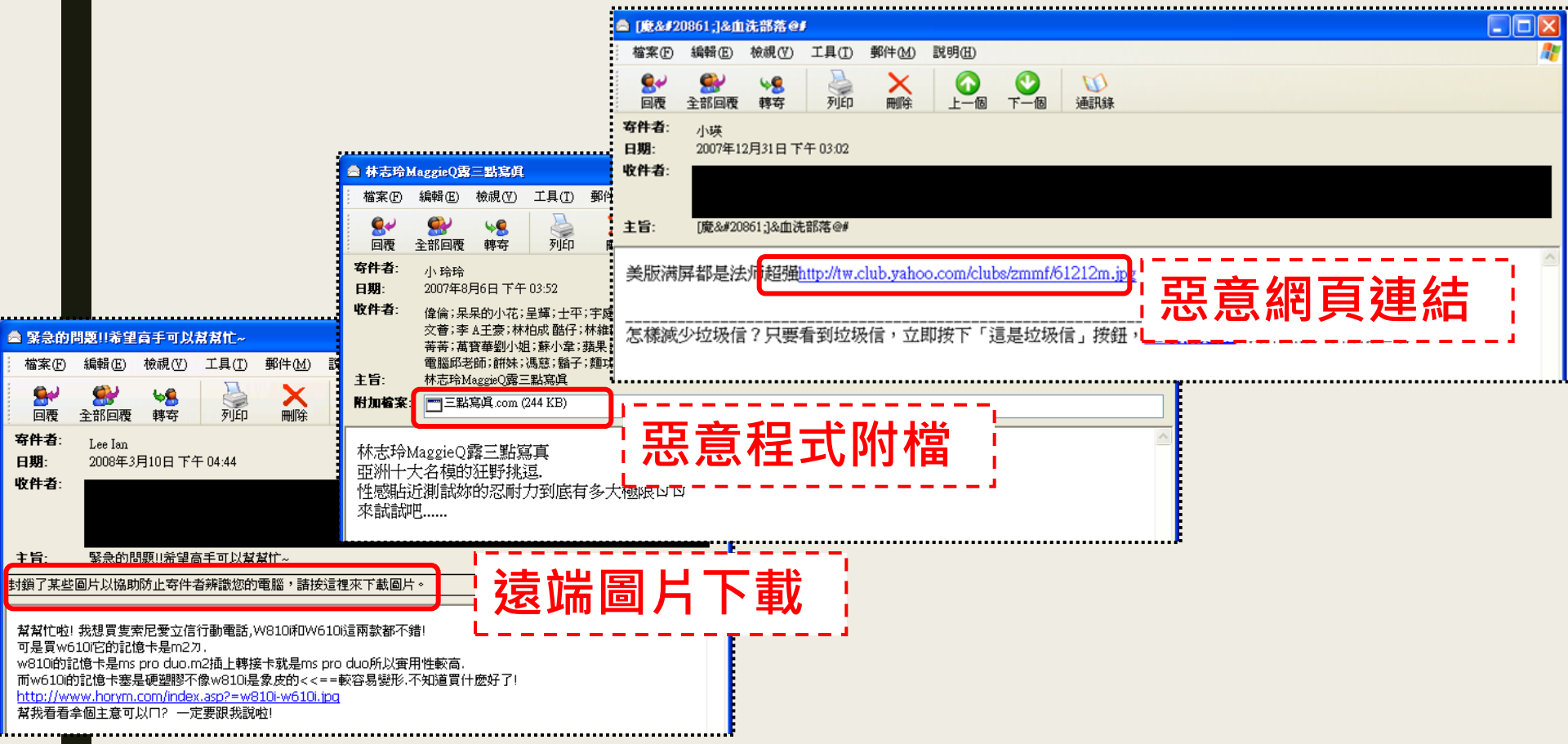
含有惡意程式附件 範本


OFAC NEW LISTS OF BLACKLISTED AGENTS - 郵件 (HTML)
檔案
郵件
刪除
回覆
全部回覆
轉寄
移動
分類
待處理
翻譯
顯示比例
OFAC NEW LISTS OF BLACKLISTED AGENTS
General Information
http://[redacted]/cjxnedt+
按一下以追蹤連結
VIEW
DOWNLOAD
Ârlista KÃ©rÃ©s.doc [Compatibility Mode] - Word
FILE
HOME
INSERT
DESIGN
PAGE LAYOUT
REFERENCES
MAILINGS
REVIEW
VIEW
%PDF-98923813.39892381398923813=
PAGE 1 OF 1
2 WORDS

電子郵件使用安全應有的認知

社交工程電子郵件的陷阱

- 郵件中惡意連結與程式附檔
- 郵件中的遠端圖片下載（與ActiveX）



開啟郵件...
點擊郵件中的連結...
開啟郵件中的附檔...

您可能已經明白了

不要點擊連結與隨意開啟這些附檔，

但您可能還是疑惑

為什麼開啟郵件也算違規？

為何要求不能「開啟郵件」？

- **似乎只要不開郵件附件和不點擊連結，就不會中招...**

→但有些惡意程式是利用ActiveX功能來執行的

→由於您的電子郵件可能是HTML格式，而HTML可以撰寫ActiveX，所以您只要瀏覽電子郵件，就觸發ActiveX執行！

載入郵件圖片是危險的嗎？

- 開啟信件，信件中圖片有可能夾帶木馬、後門程式等。
- 信件中的圖片若有顯示出來就有可能中毒。

將惡意程式設定檔暗藏在 JPG 影像中

- 漂亮的落日風景

只要一張圖片就能駭掉你的電腦

每日頭條

首頁 | 健康 | 娛樂 | 時尚 | 遊戲 | 3C | 親子 | 文化 | 歷史

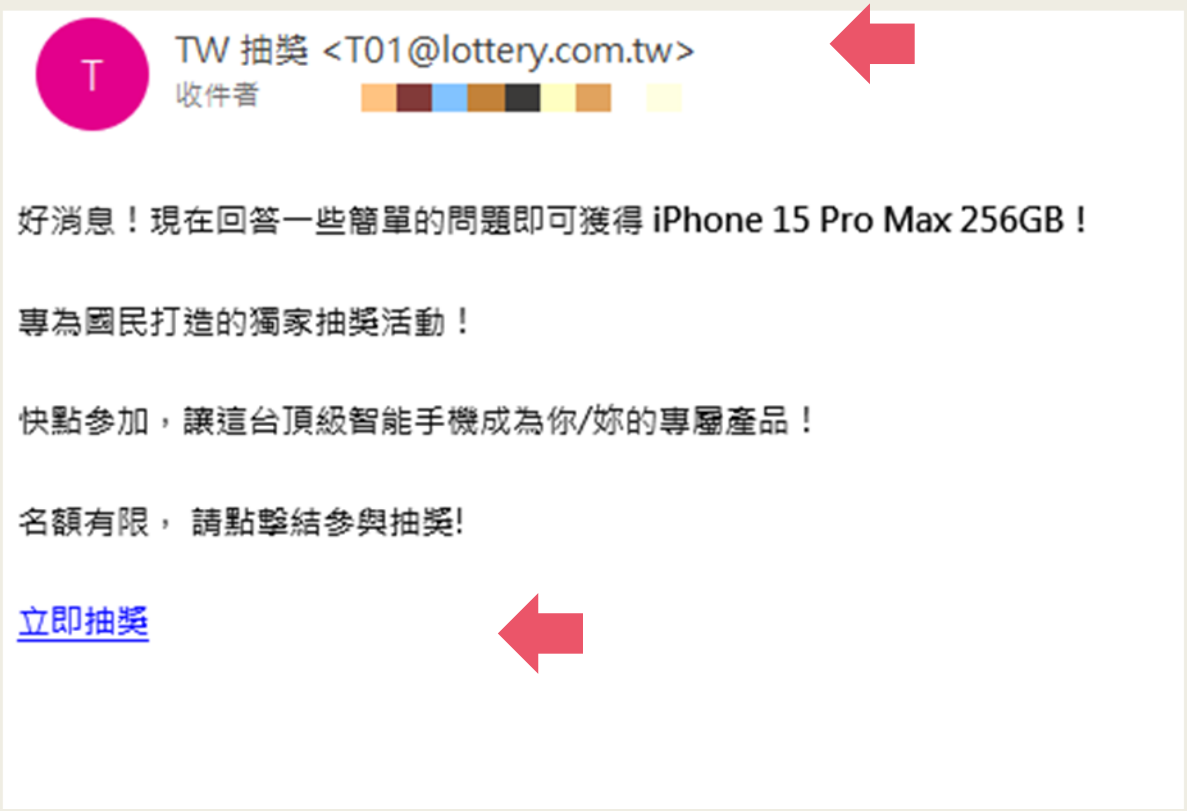
廣告圖片像素隱藏惡意代碼，「Stegano」波及歐洲五國新聞網站用戶

據外媒報導，在過去的幾個月里，數以百萬計的用戶可能已經在訪問主流新聞網站時遭到惡意廣告攻擊。攻擊者在網頁廣告圖片的單個像素中嵌入惡意代碼。

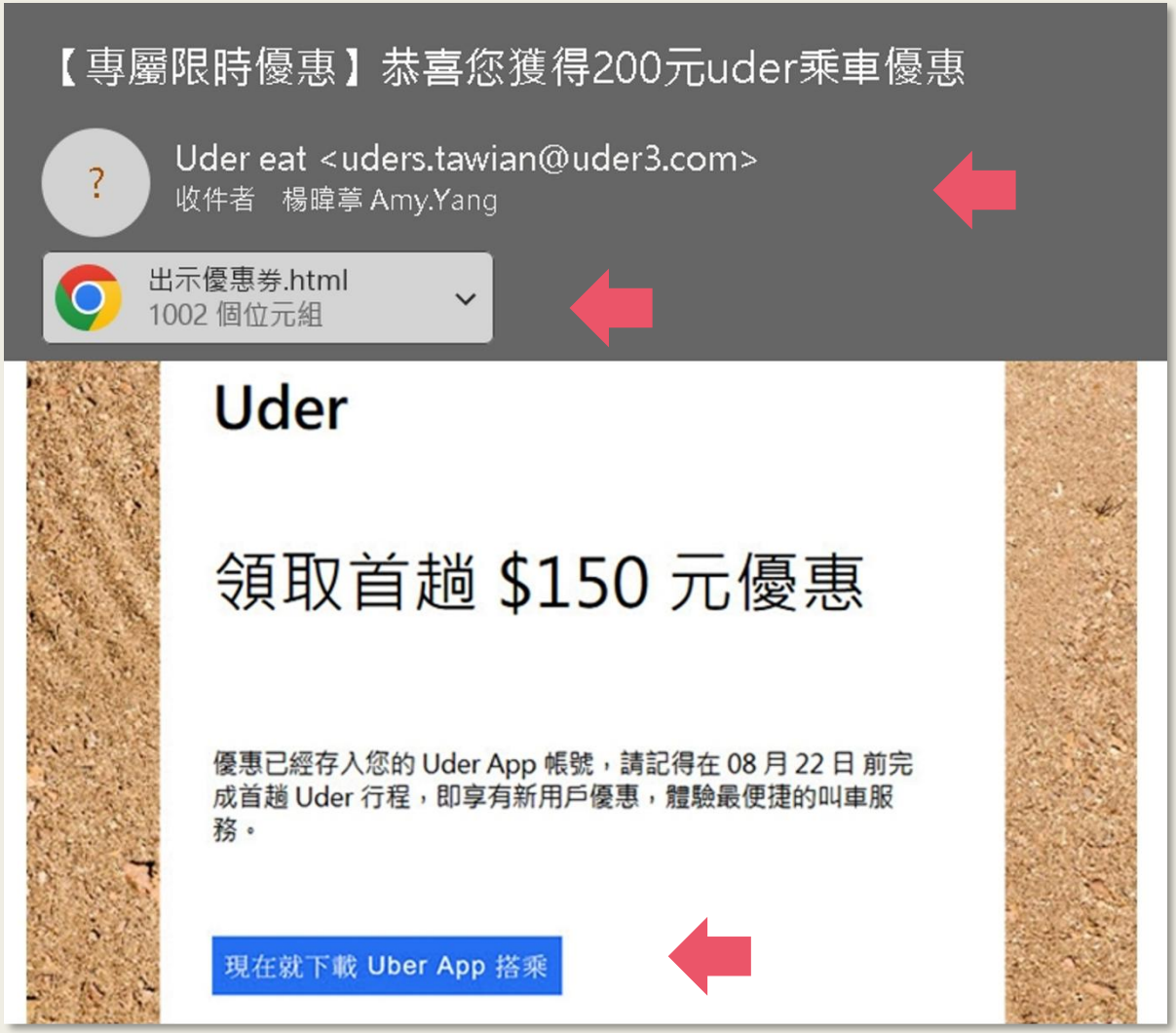
常見的社交工程郵件範例

電子郵件社交工程模擬範例-1

繁中：抽獎活動！贏取 iPhone 15 Pro Max 256GB 限量五台!



電子郵件社交工程模擬範例-2



電子郵件社交工程模擬範例-3

訂單已確認(訂單編號: ODSCE201723758124)

購物中心 [system@shopping-market.com.tw]

至: Leo_chang

附件: 訂購清單.doc (1 KB) [開啟為網頁]

2017年6月2日 下午 02:56

親愛的 顧客 您好：

我們已收到您的訂購資訊，感謝您的訂購。
本信函只是系統通知已收到您的訂購訊息、並供您再次自行核對之用，謝謝。

訂單資訊...

提醒您！
我們不會以電話通知更改付款方式或要求改以ATM重新轉帳。
亦不會委託廠商以電話通知變更付款方式或要求提供ATM匯款帳號。
請確認附件資訊是否正確，如果有誤請點選連結告訴我們。

電子郵件社交工程模擬範例-4

繁中：行人地獄惡名 交通部要求請做一舉動

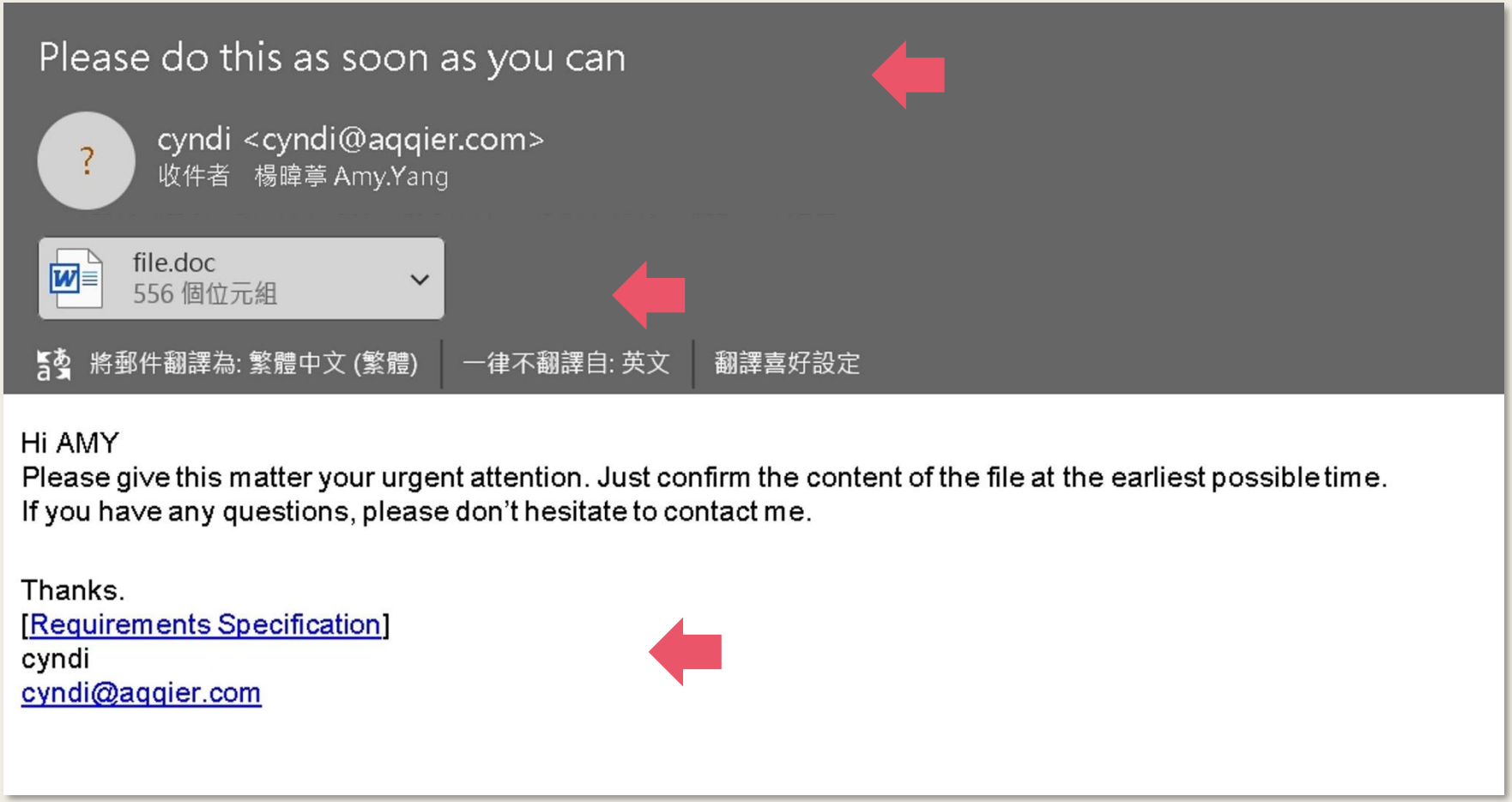
聯合新聞网 <und@udn.com.tw>
收件者

圖文說明.html
11 KB

「日本兒童過馬路，為什麼要舉手打招呼？有人以為是有禮貌。」

其實是因為日本的行人車禍死亡過去也很多，即使到現在仍是不低，因此過馬路為了安全起見就要大家舉手打招呼。

電子郵件社交工程模擬範例-5



行動裝置的社交工程

行動裝置有檢查過嗎?

你的手機或平板有好好檢視過嗎?

駭客攻擊行動裝置已然是主要。

落實手機安全管理

- 密碼強度要夠
- 不與他人共用私人手機
- 只從官方來源取得App程式
- 判斷App程式所要求的權限合理性
- 仔細觀看所有的提示訊息
- 遇到索取帳號密碼的情形時要特別提高警覺
- 小心App中的指示 (點連結、安裝其他App...)

收信軟體與相關安全性設定

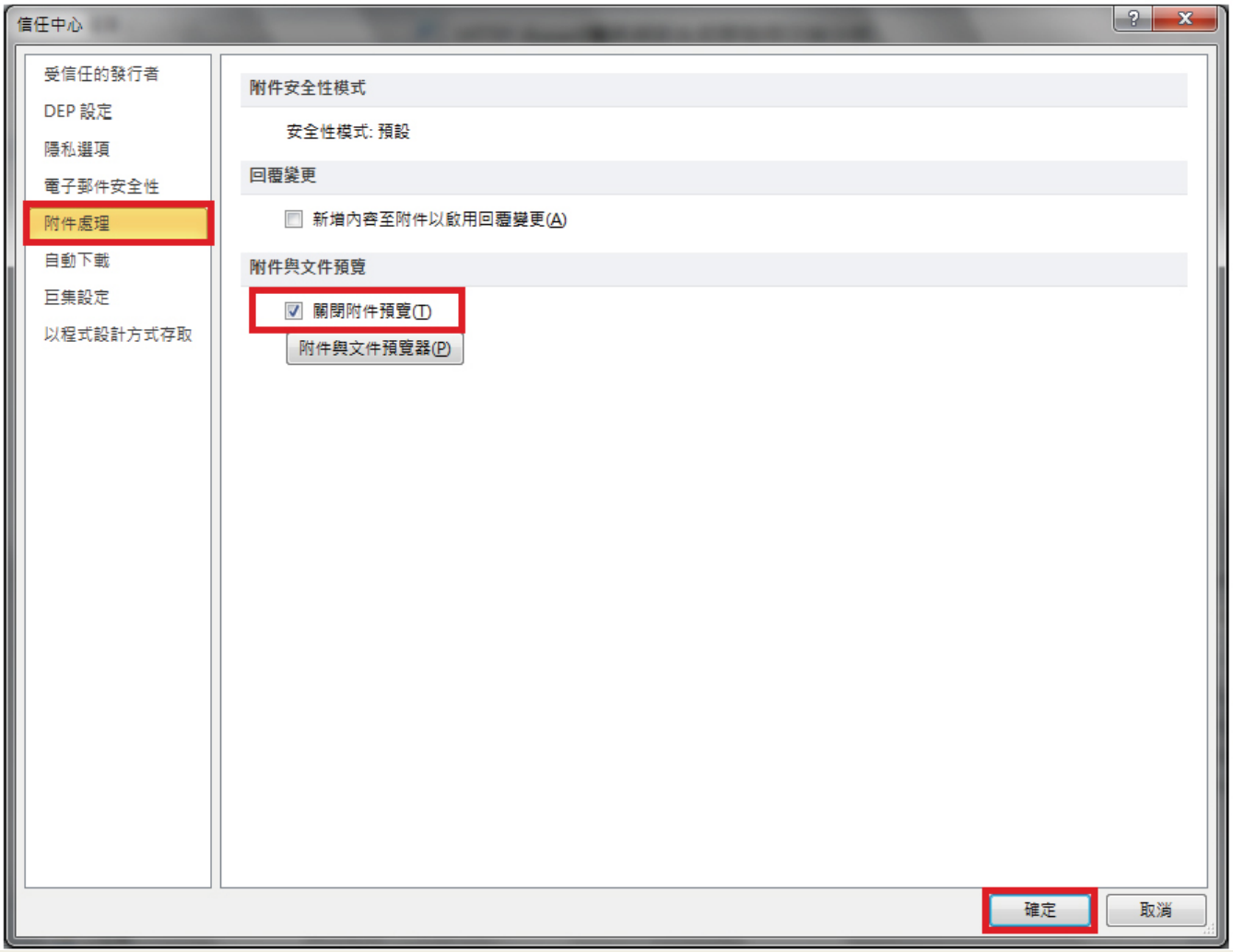
收信軟體安全設定

以微軟的 Outlook 收信軟體為例，
建議進行以下安全性的設定：

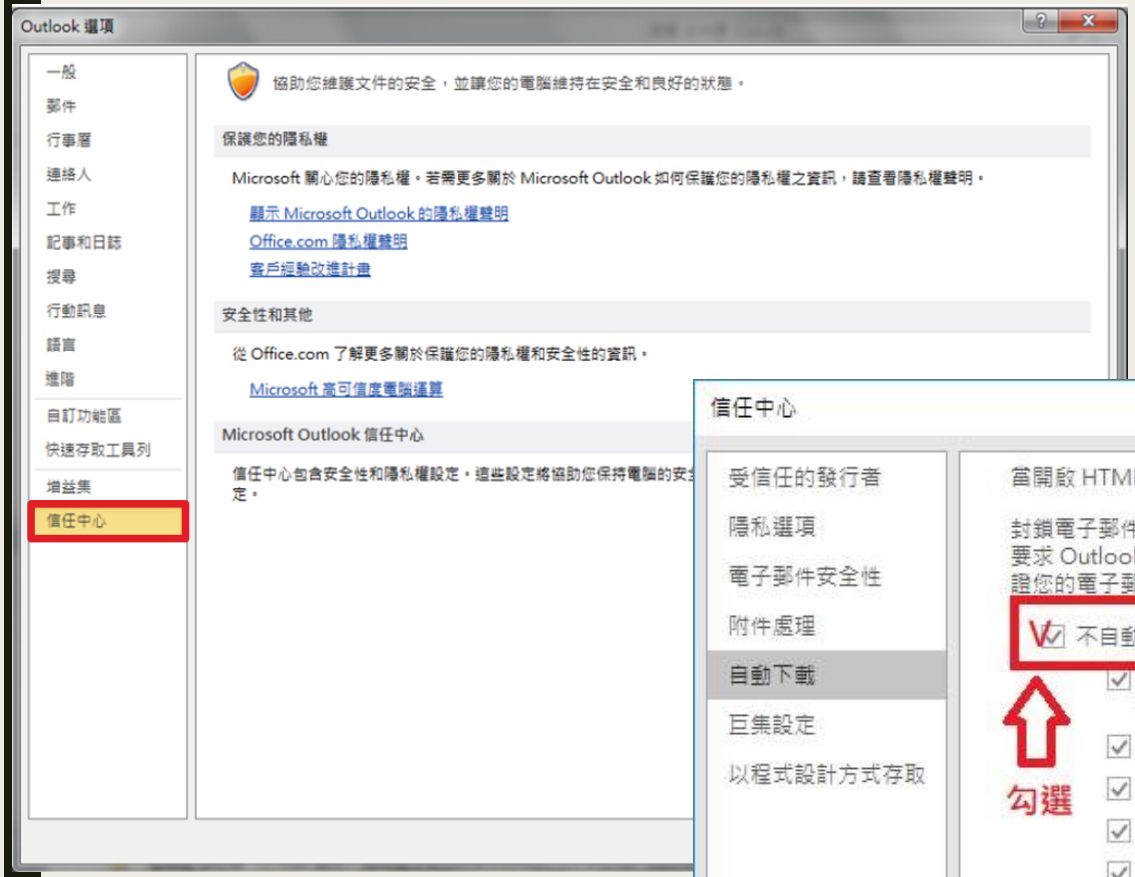
- **關閉「郵件預覽」「附件預覽」**
- **關閉「自動載入郵件圖片」**
- **以「純文字讀取」郵件**
- **設定「不要自動回覆讀信回條」**

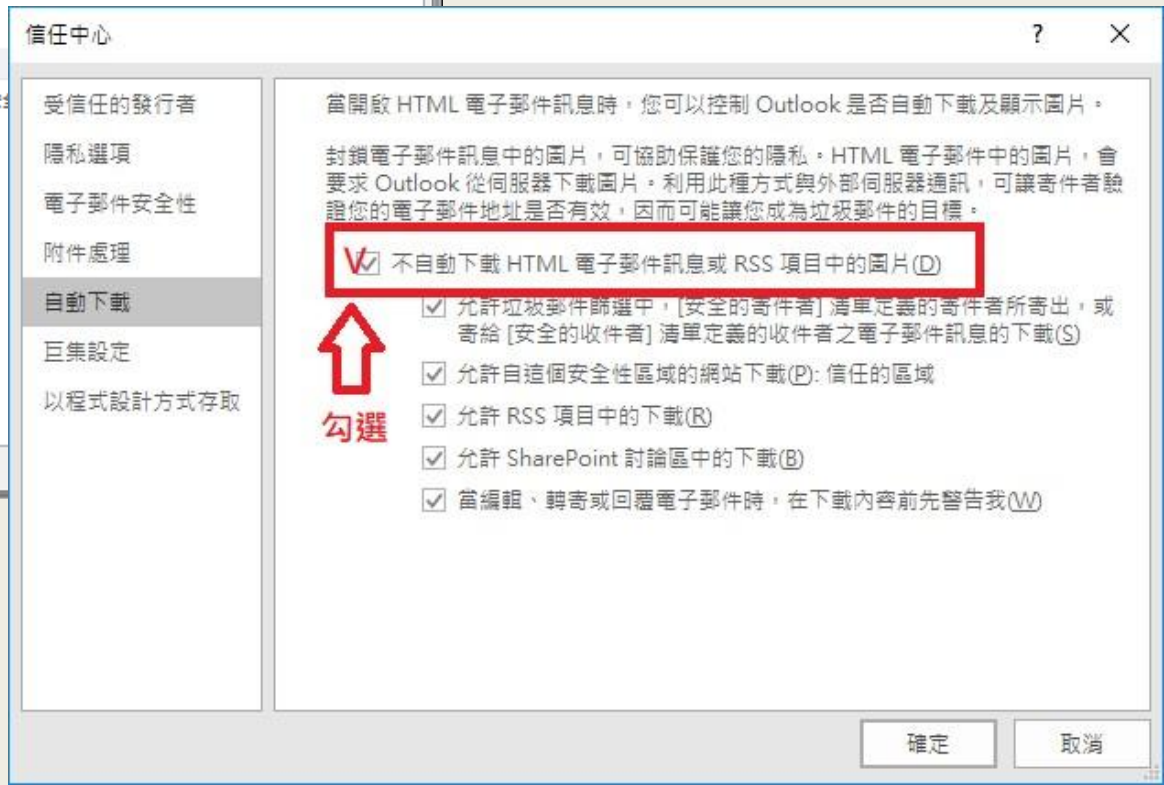
收信軟體安全性設定-關閉郵件預覽

收信軟體安全性設定-關閉附件預覽

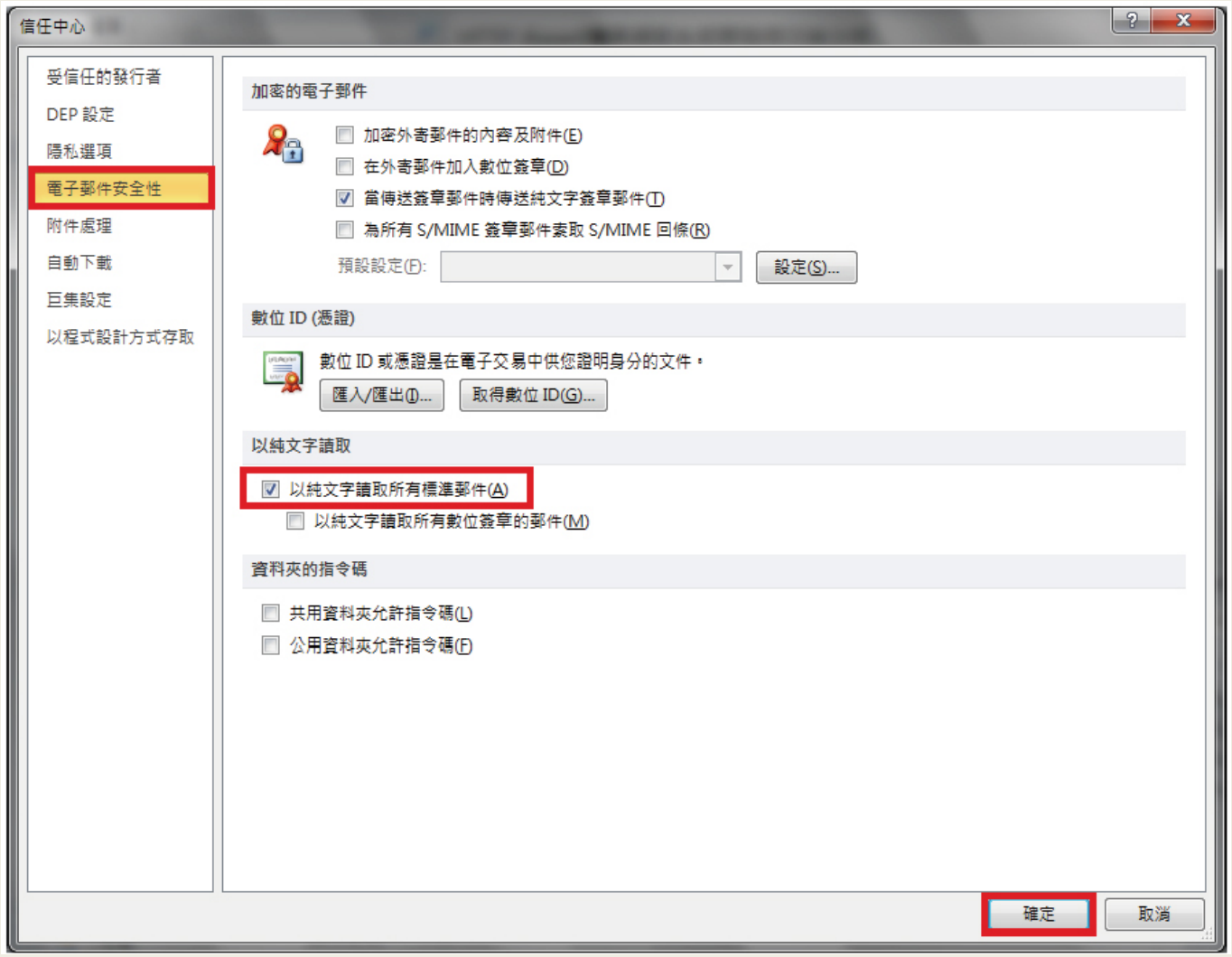


關閉信件自動下載圖片及其他內容

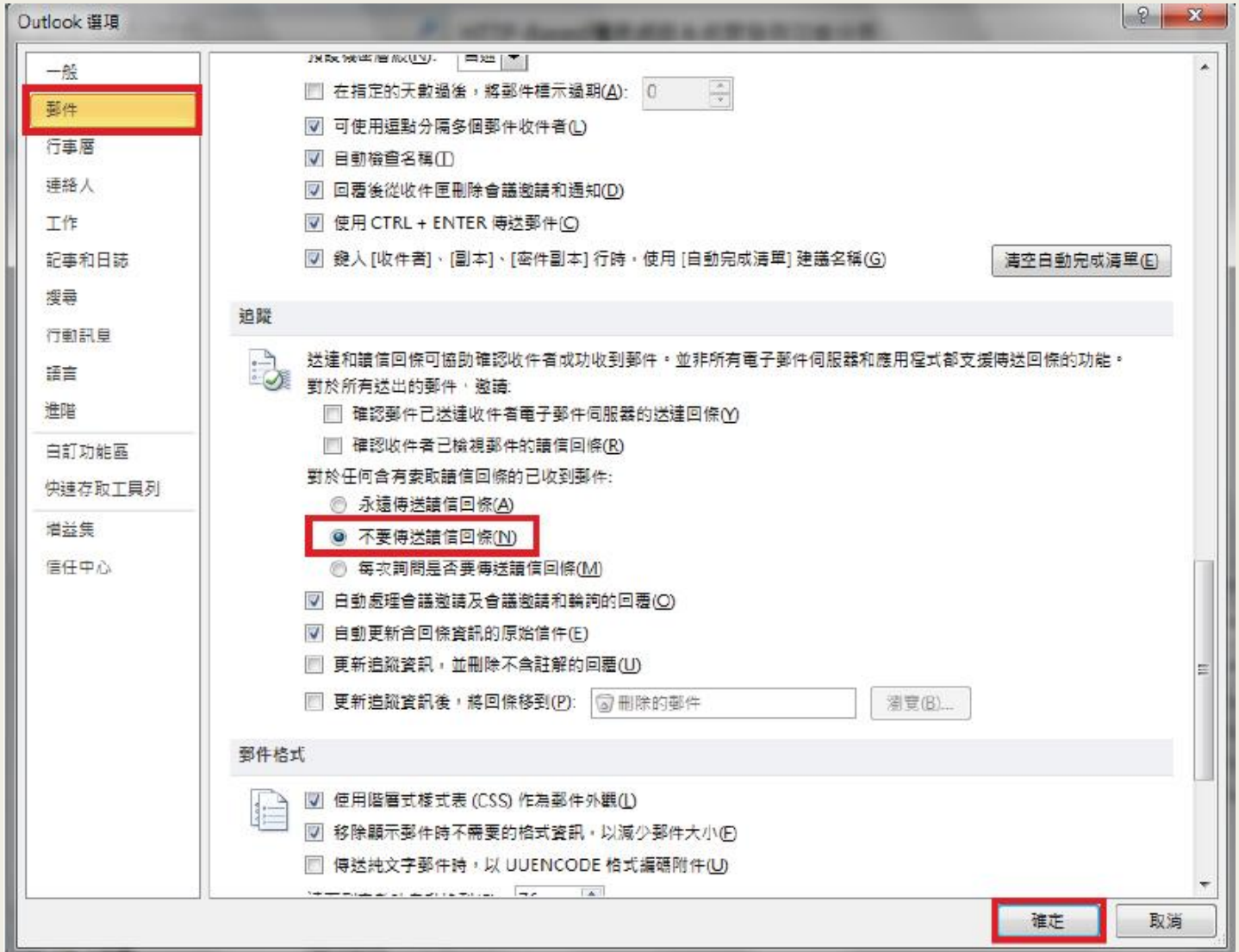




收信軟體安全性設定-以純文字讀取郵件



收信軟體安全性設定-不自動回覆回條

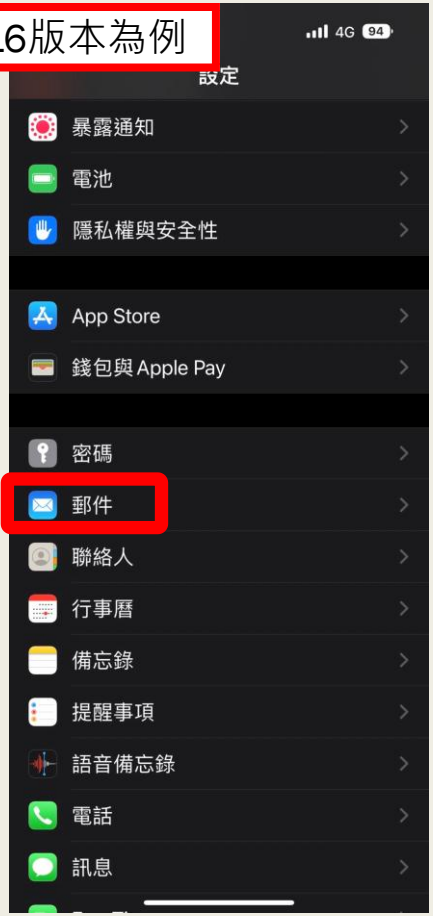


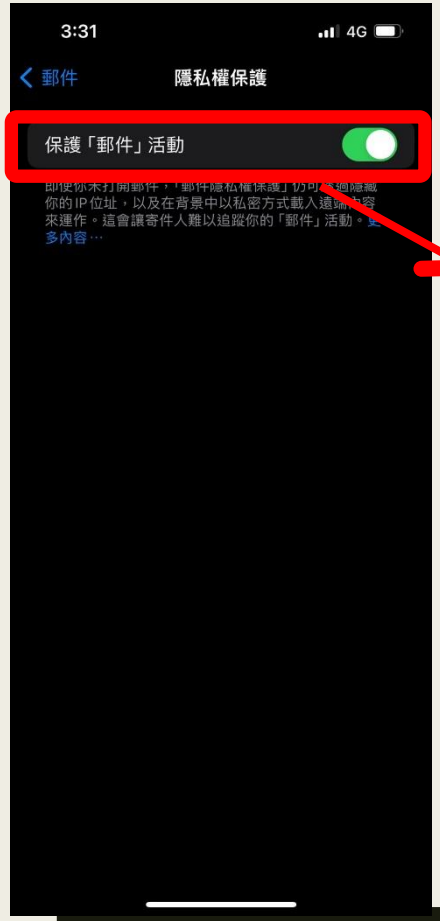
iOS / Android 郵件圖片自動載入設定

- 2017年 iOS 版本更新，關閉了預設自動載入圖片，改為需手動載入郵件圖片
- Android 一般都是預設不自動載入郵件圖片，但可能會依手機廠牌而有差別

iPhone 郵件安全性設定-停用自動顯示圖片

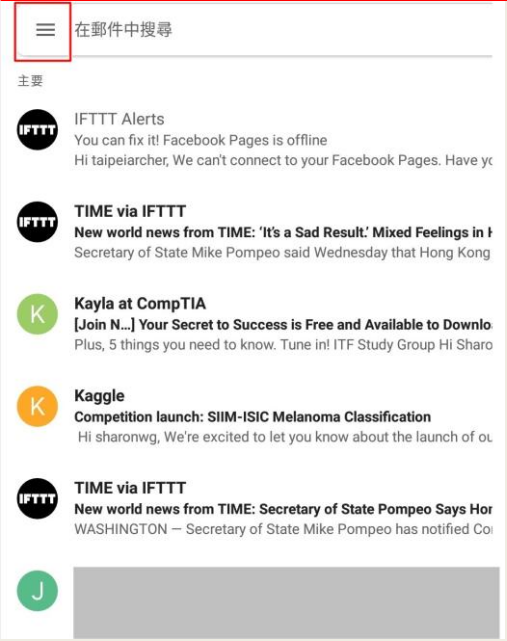
以IOS16版本為例

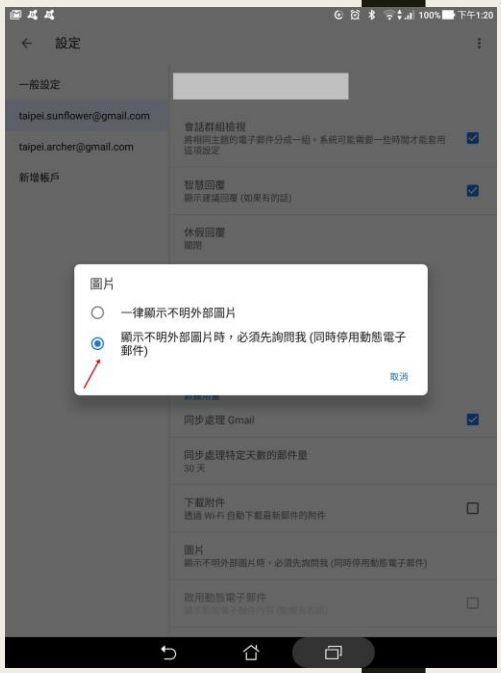




Android 郵件安全性設定-停用自動顯示圖片

以Android11&Gmail2022.12.25版本為例





關於社交工程郵件我們可以..

- **不上鉤**：收到標題吸引人的郵件，務必停看聽。
- **不打開**：不隨便打開Email附件檔案。
- **不點擊**：不隨意點擊Email中的連結網址。
- **要確認**：打開Email前要確認寄件者身份。
- **請勿使用公司Email註冊**個人社群帳號(FB、Twitter等)及個人電子帳單或是其他非公務使用之網站；如是公務上所需，則密碼也請勿設定成跟公司網路登入之相同密碼。

簡短重點項目

- 請勿開啟任何陌生人所寄來的電子郵件。
- 就算是認識的人也請勿隨意點選「超連結」。
- 開啟任何郵件的附件檔前，請記得「另存新檔」掃毒後再開啟。

報告完畢