認識惡意信件的危害與防範對策

網路管理組　王裕仁

愛護地球，
請在電腦觀看減少列印

2016/4/14

大綱

- 介紹惡意信件的種類
- 認識最近新興的勒索信
- 惡意信件的防範對策
  - 郵件安全設定
  - 離線備份與雲端備份

惡意信件的種類

- 廣告信 / 垃圾信
- 病毒信
- 含有木馬的信件
- 詐騙信 / 釣魚信
- 勒索信

廣告信 / 垃圾信

廣告信由來已久，自有 email 以來就有廣告信，本校已有廣告信攔截系統。

病毒信

- 病毒信是利用郵件軟體或電腦系統的漏洞，自我複製並感染其他電腦。
- 本校已有病毒信過濾系統。
- 由於郵件伺服器已經有病毒信過濾系統，且大部分的電腦都有安裝防毒軟體，所以近幾年已經較少大規模感染的事件。

含有木馬的信件

- 木馬程式又稱特洛伊木馬，它是一種惡意程式，與病毒最大的不同是它不會自我複製，通常需要使用者點擊連結或附檔。
- 被植入木馬的電腦，駭客就可以遠端遙控您的電腦，可以側錄您的帳號密碼、竊取電腦中的檔案或是將您的電腦當作跳板去攻擊別人。

木馬的例子 (一)

傳送路徑:

OA/TKU

"亞洲研究所"
<tijx@oa.tku.edu.tw>

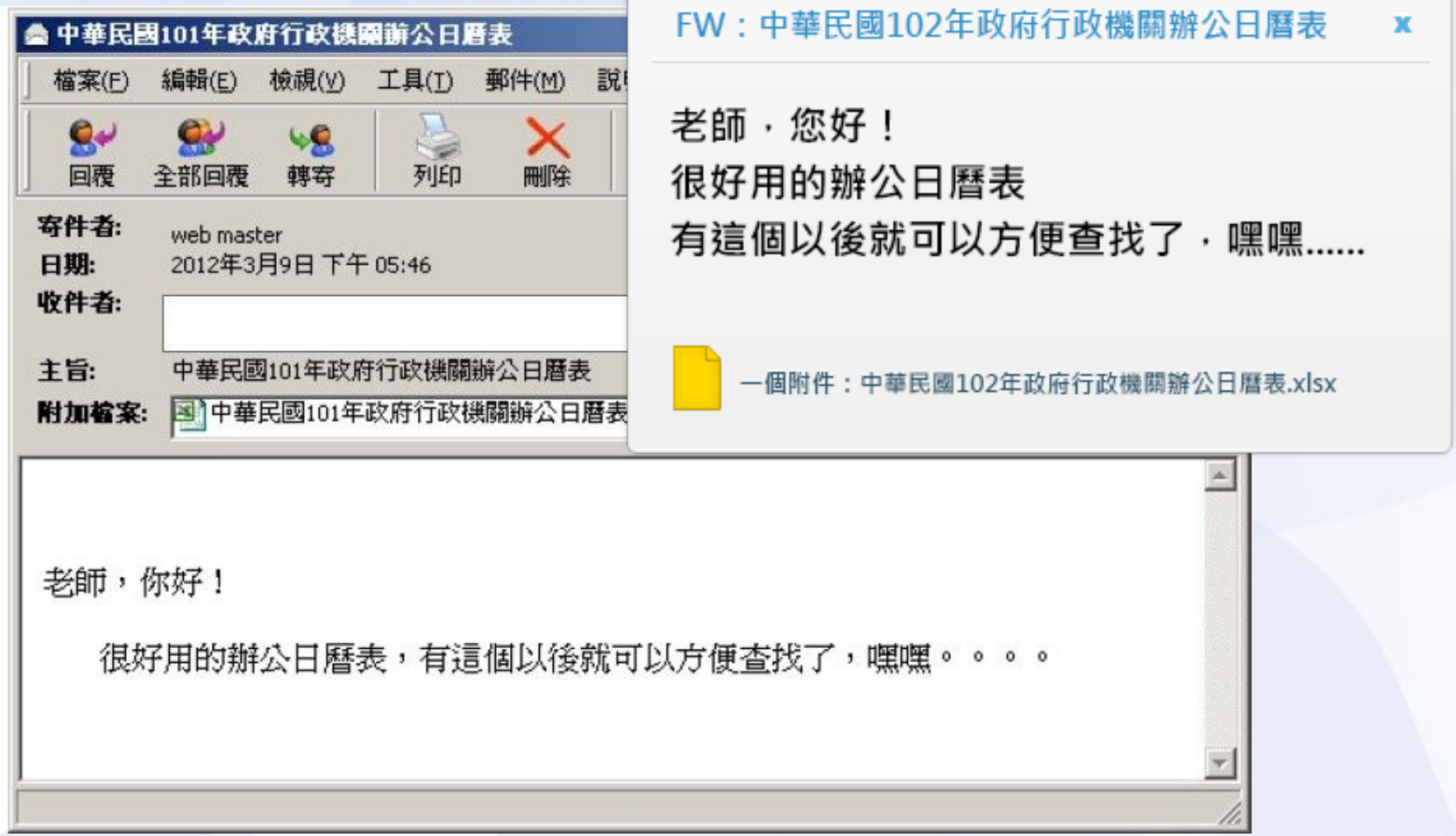
上午 11:28 今天

收件者:<ctsay200@yahoo.com.tw>
副本抄送:
主旨:轉寄：公布102年度職員年資休假名單及可休天數，請 查照。

=

附件： 附加檔-102年度職員年資假名單.rar 614k 位元組 **開啟**

木馬的例子 (二)


中華民國101年政府行政機關辦公日曆表
檔案(F) 編輯(E) 檢視(V) 工具(T) 郵件(M)
回覆 全部回覆 轉寄 列印 刪除
寄件者: web master
日期: 2012年3月9日 下午 05:46
收件者:
主旨: 中華民國101年政府行政機關辦公日曆表
附加檔案: 中華民國101年政府行政機關辦公日曆表
老師，你好！
很好用的辦公日曆表，有這個以後就可以方便查找了，嘿嘿。。。。
FW：中華民國102年政府行政機關辦公日曆表
老師，您好！
很好用的辦公日曆表
有這個以後就可以方便查找了，嘿嘿.....
一個附件：中華民國102年政府行政機關辦公日曆表.xlsx

詐騙信 / 釣魚信

詐騙信 (釣魚信) 件是由駭客假冒他人的名義發出偽造的信件，並提供假的連結或附檔，誘騙使用者開啟附檔、連到惡意網站或誘騙使用回覆帳號密碼，達到入侵電腦或騙取個資的目的。

詐騙信和廣告信的不同

- 廣告信很煩人但是無害，只是想推銷商品而已。

- 詐騙信經過精心設計的郵件標題、寄件者、郵件內容、附件檔名，將惡意郵件偽裝成正常郵件，誘使受害者開啟連結或附檔，達到詐騙的目的。

釣魚信的例子 (一)

系統管理員 <ke.ptgg@baidui.com>

2015/06/02 08:00

Email緊急維護重要通知！

收件人:

1

顯示圖片

Email緊急維護重要通知！

維護原因: 公司辦公自動化（Webmail）自運行以來，不斷優化完善。爲提高辦公效率，實現無紙化辦公，公司將全面推進辦公自動化（Webmail）的使用。現對所有用戶郵箱進行版本升級！由於您長期未驗證郵件係統賬號信息,導致係統無法識別信息，或超過三個月未登錄!爲保證正常使用（現需要對郵箱進行升級並需要重新采集用戶信息)

維護時間: 本次升級檢測爲期7-15天，爲此給你帶了不便的地方，敬請理解。

注意事項: 爲確保合理使用Webmail系統資源，若是收到此通知當天下班前沒有前往升級或者校驗用戶信息,后台將自動識別此用戶或是無人使用的郵箱，將被自動刪除，感謝您的配合!

請點這裡進行升級

釣魚信的例子 (二)

新建立 回覆 全部回覆 轉寄 更多

緊急通知教職員/學生/員工

Universities Staff/Student/Employee Portal

收件人: undisclosed-recipients:

副本密送: 國際企業學系

親愛的：郵局認購

我們特此宣布您，您的電子郵件帳戶已超過其
存儲限制。您將無法發送和接收郵件和你
從我們的服務器，電子郵件帳戶將被刪除。為了避免這個問題，
建議您通過點擊鏈接確認您的電子郵件帳戶
如下：

http://verificationmailtwportal.webs.com/

謝謝。

(c)版權所有2013
系統管理員的管理團隊。

釣魚信的例子 (三)

台灣電子郵件管理員中心 <admin@fit.edu.tw> 2016/03/16

親愛的電子郵件使用者

親愛的電子郵件使用者

您的郵箱已超過其存儲限制由電子郵件管理員設置，您將無法接收新郵件，直到你重新驗證 它。

點擊這裡：http://formcrafts.com/a/18436?preview=true

在其他的重新驗證您的電子郵件帳戶作為目前使用的帳戶。

釣魚信的例子 (四)

垃圾桶 [清空]
外部郵件

說明
登出

From: 資訊處 網路管理組 [mailto:fk@oa.tku.edu.tw]
Sent: Monday, October 28, 2013 7:41 AM
Subject: 通 知：信箱收取信件異常，即將達到系統上限！
Importance: High

親愛的師長：

您的信箱使用空間已經達到系統上限的95%， 系統會主動以簡訊通知您使用空間即將不足，空間不足將導致無法正常收取一切來信。為避免影響您正常使用 信箱提供的服務，建議您立即登入網址http://webmail.tku.edu.tw/posmat_2g 增 加

淡江大學資訊處　網 路管理組
網頁郵件登入地址：http://webmail.tku.edu.tw

webmail.tku.edu.taiwans.tw/tku_mail/webmail.asp

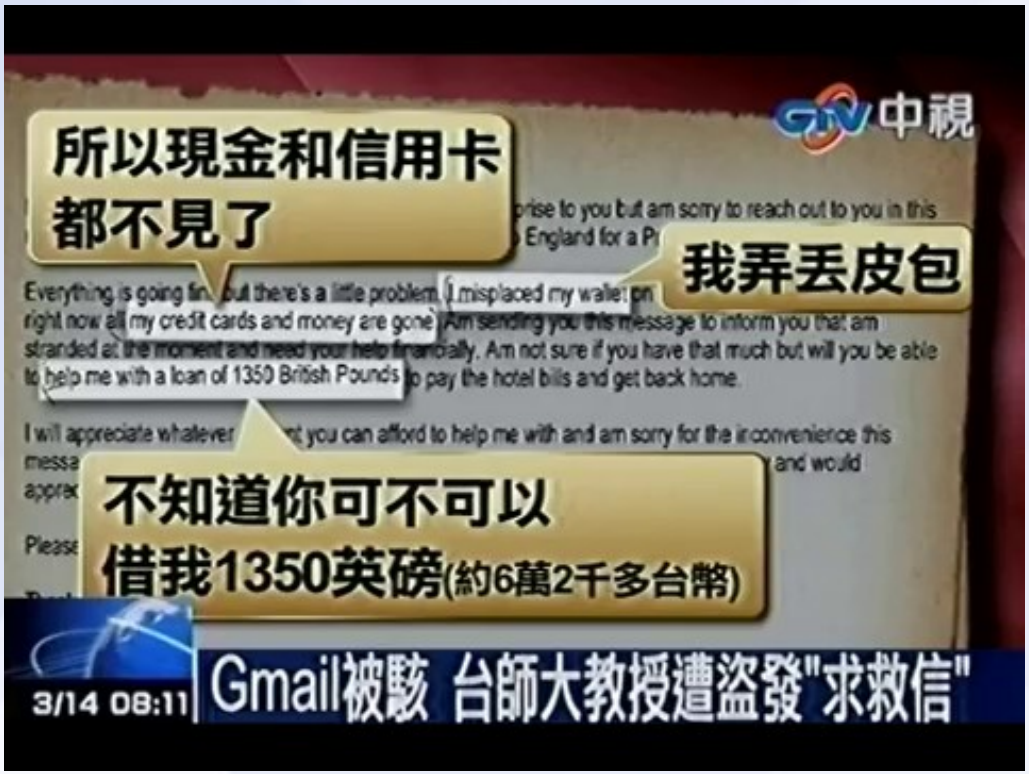
中了釣魚信或木馬會怎樣

- 電腦被植入惡意程式
- 洩漏個資
- 被冒用名義寄詐騙信，使更多人受害
- 被詐騙金錢 / 害你的親朋好友被騙錢

一個受駭(害)者的案例

Gmail 被駭 台師大教授遭盜發「求救信」

https://youtu.be/AKLhn3e2CzY



認識最近新興的勒索信

中研院也受害！勒索病毒侵萬部電腦

https://youtu.be/c8JWBx1tE24

看到這些畫面表示您已經被勒索了

認識勒索信

- 一旦點了信中的連結或附檔，您的電腦就會被植入勒索 (流氓) 軟體，然後把電腦中的資料檔全部加密。
- 每個檔案用不同的金鑰以 AES-256 加密。
- 每個檔案的金鑰再以 2848bit 的 RSA 加密。
- 需匯一定金額的比特幣給作者才能解密。
- 變種頻率很高，多半是不同集團做的。

認識勒索信 (續)

- 付錢給勒索軟體作者並不是一個好的做法，因為沒人能保證付錢之後檔案可以救回來。
- 以目前個人電腦的運算能力，以暴力破解 2048bit 的 RSA 加密約需 10^{160}~10^{210} 年。

無量大數 = 10^{68}

googol = 10^{100}

目前宇宙年齡約 1.5x10^{10} 年

黑暗中的一線曙光

- 卡巴斯基的 Ransomware Decryptor 網站收錄了之前警方破獲勒索集團的加密金鑰。
- 涵蓋 CryptoLocker 、 CoinVault 及 Bitcryptor 。

- 網址： https://noransom.kaspersky.com

惡意信件的防範對策

廣告信及病毒信攔截系統

- 被攔截的信多半是有問題的信，別好奇去開

寄給 900052@mail.tku.edu.tw 的疑似垃圾郵件列表

報告產生時間: 03/28/16 06:00:00

使用說明請參閱信件尾端。

傳送	核准	日期	大小	寄件人	主旨
傳送	核准	2016/03/28 18:14	4k	[redacted]	[redacted]
傳送	核准	2016/03/28 18:58	36k	Reid Colon	FW: Overdue Incoices
傳送	核准	2016/03/28 23:23	36k	Sheryl Nolan	FW: Overdue Incoices
傳送	核准	2016/03/29 02:57	4k	[redacted]	[redacted]
傳送	核准	2016/03/29 04:10	4k	[redacted]	[redacted]
傳送	核准	2016/03/29 05:33	4k	rosemarykirk@post.com	Microsoft Internet E-mail lottery Awa

如何防範詐騙信

- 不要開啟來路不明信件的附檔或連結。
- 不是所屬業務的信件請提高警覺。
- 使用電子郵件應有的警覺性觀念：
  - 我為何會收到這封信？
  - 我是不是真的有必要開啟附件或點選連結？

  如有疑問可向發信者查證
- 不要太八卦，看到怪怪的信就不要再轉寄 !!

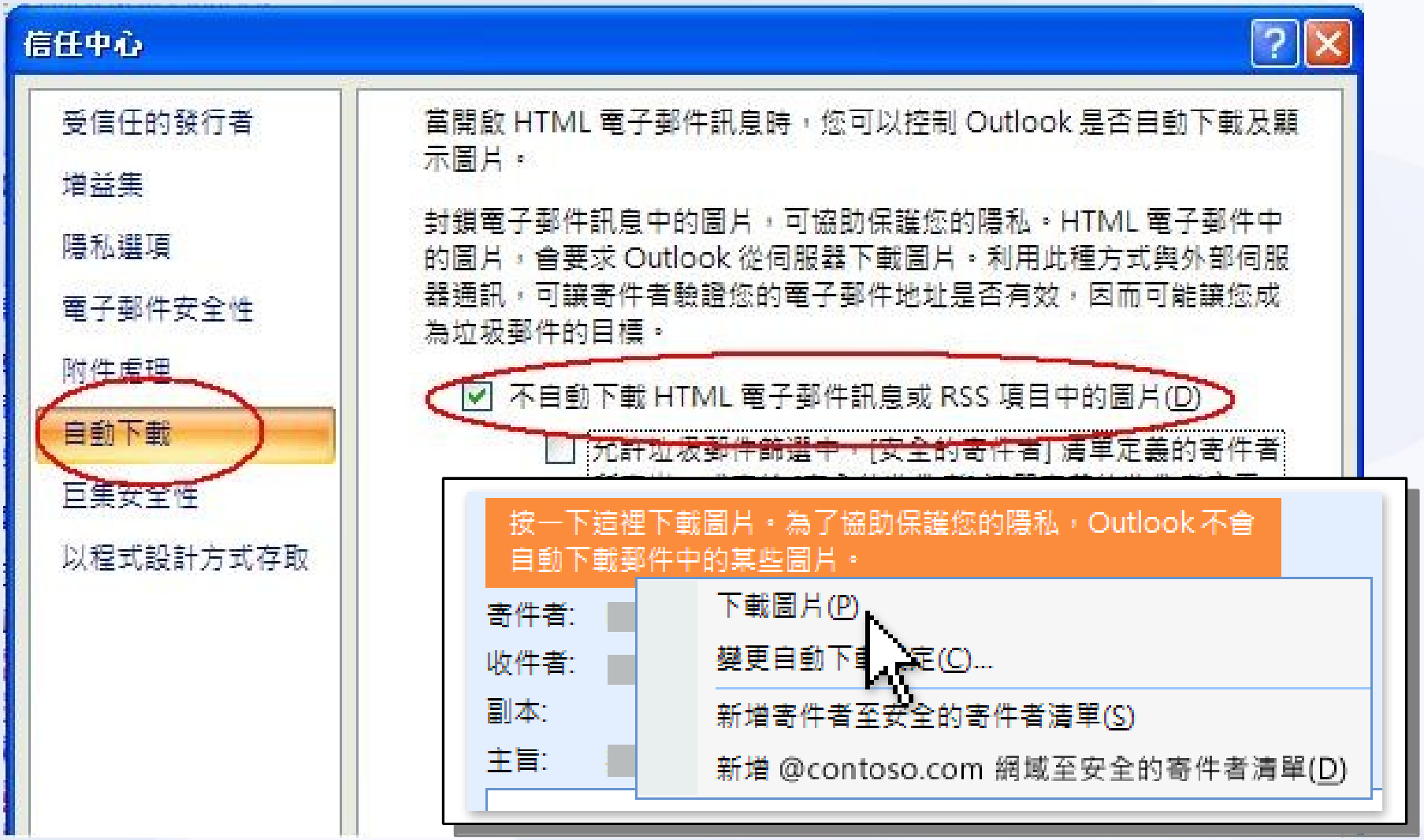
詐騙信的特徵

- 吸引人的主旨
- 過於聳動或緊急的主旨
- 威脅利誘的字眼
- 陌生人或極少來往對象的來信
- 需要輸入敏感資料的信件

注意！ 寄件者是可以偽造的 !!

webmail 的安全設定

收信軟體的安全設定


信任中心
受信任的發行者
增益集
隱私選項
電子郵件安全性
附件處理
自動下載
巨集安全性
以程式設計方式存取
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。
封鎖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(D)
按一下這裡下載圖片。為了協助保護您的隱私，Outlook 不會自動下載郵件中的某些圖片。
寄件者:
收件者:
副本:
主旨:
下載圖片(P)
新增寄件者至安全的寄件者清單(S)
新增 @contoso.com 網域至安全的寄件者清單(D)

離線備份與雲端備份

- 離線備份：將檔案備份至隨身碟或磁帶上，並把隨身碟或磁帶從電腦上移除。

- 雲端備份：將檔案同步至 Google Drive、Dropbox 或 One Drive 等雲端硬碟。
雲端硬碟多有提供「檔[illegible]的機制，可以將檔案[illegible]

請留意本校個資規範

教育部社交工程演練

提醒您，教育部將於四月下旬開始進行本年度的社交工程演練，期望大家都能明智的避開，不要上當。

感謝各位的參與 !!