電子郵件暨社交工程攻擊趨勢與防護

課程綱要

- 網路安全威脅綜覽
- 社交工程攻擊趨勢
- 電子郵件安全管理
- 有效防護實作討論

課程綱要

- 網路安全威脅綜覽

網路安全威脅綜覽

- 台灣整體網路威脅位居**全球網路威脅報告排名第九**，前三名分別為美國、中國與印度。
- **垃圾郵件攻擊**大幅增加，與前年相比躍升8個名次，成為全球第四大受此影響的地區。
- 台灣的針對性攻擊87%鎖定**中大型企業251~2500人**（相較於全球，同規模的企業僅佔整體針對性攻擊的31%）
- **零售業與製造業**為台灣兩大容易遭受針對性攻擊的產業

Organisation Size	Percentage
1-250	13.33%
251-500	6.67%
1501-2500	80.00%

Industry	Percentage
Wholesale	50.00%
Manufacturing	45.83%
Finance, insurance & Real Estate	4.17%

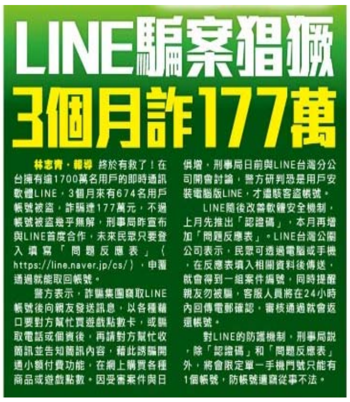
課程綱要

- 社交工程攻擊趨勢

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
- 圖片內含惡意程式
- 偽裝修補程式
- 即時通

(LINE, Yahoo, Skype...)



LINE騙案猖獗
3個月詐177萬

林志青・報導 終於有救了！在台擁有逾1700萬名用戶的即時通訊軟體LINE，3個月來有674名用戶帳號被盜，詐騙逾177萬元，不過帳號被盜幾乎無解，刑事局昨宣布與LINE首度合作，未來民眾只要登入填寫「問題反應表」（https://line.naver.jp/cs/），申覆通過就能取回帳號。

警方表示，詐騙集團竊取LINE帳號後向親友發送訊息，以各種藉口要對方幫忙買遊戲點數卡，或騙取電話或個資後，再請對方幫忙收簡訊並告知簡訊內容，藉此誘騙開通小額付費功能，在網上購買各種商品或遊戲點數。因受害案件與日俱增，刑事局日前與LINE台灣分公司開會討論，警方研判恐是用戶安裝電腦版LINE，才遭駭客盜帳號。

LINE隨後改善軟體安全機制，上月先推出「認證碼」，本月再增加「問題反應表」。LINE台灣公關公司表示，民眾可透過電腦或手機，在反應表填入相關資料後傳送，就會得到一組案件編號，同時提醒親友勿被騙，客服人員將在24小時內回傳電郵確認，審核通過就會返還帳號。

對LINE的防護機制，刑事局說，除「認證碼」和「問題反應表」外，將會限定單一手機門號只能有1個帳號，防帳號遭竊從事不法。

社交工程可應用之弱點

- 助人的天性
- 同情心
- 好奇心
- 缺乏警覺
- 過於相信別人

有下列症狀的同仁請注意了

- 太有正義感
- 太有愛心
- 好奇寶寶
- 太容易被唬

不用打:
0800XXX000

社交工程常應用之題材

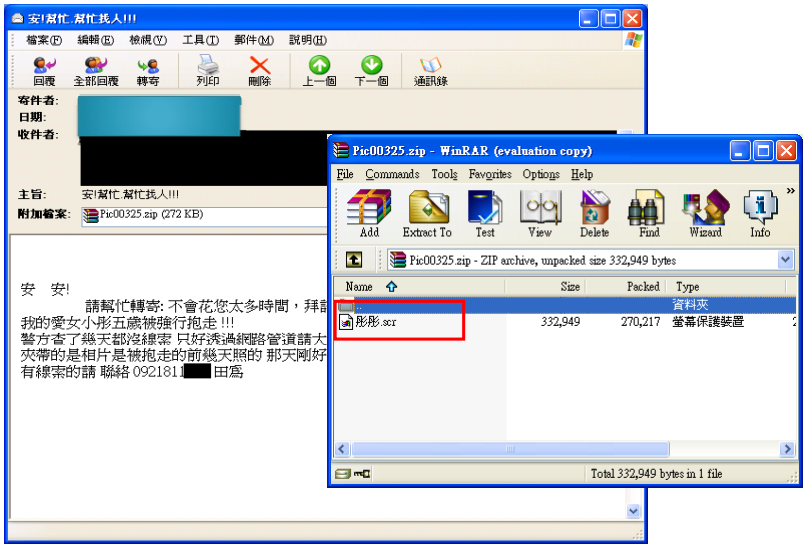
- **政治**
- **色情**
- **休閒**
- **贈品、抽獎**
- 影音媒體
- 業務職務相關
- 系統管理

電子郵件社交工程手法

惡意郵件種類

- **廣告信件**
  - 廣告信件除了浪費使用者時間外，至少不會產生直接且立即的危害 。
  - 防制機制：Anti-Spam 。
- **病毒信件**
  - 雖然病毒程式對於電腦系統會產生實質破壞，然而藉助於防毒軟體技術的進步，目前電腦病毒的威脅對於一般已安裝防毒軟體的使用者而言，屬於可控制的風險。
  - 防制機制：防毒軟體
- **釣魚（Phishing）信件**
  - 目前最流行的釣魚目的，多是以竊取使用者資料並且實質獲利為主。
  - 防制機制：安全意識與概念。
- 木馬（Trojan）信件
  - 木馬程式，因為屬於主動式攻擊行為，一旦電腦遭受入侵，立即面臨資料外洩風險。
  - 防制機制：防毒軟體 。
- 網頁綁架
  - 點選惡意連結後，開瀏覽器首頁遭置換或自動彈跳出廣告或不雅頁面。
  - 防制機制：防間諜軟體 。

很多人會開啟觀看和熱心地轉寄...



結果是……

駭客散佈連接YouTube假網址誘使用戶中毒

轉寄好友 列印

日專電）英國SophosLabs全球網路安全研究中心今天警告網路用戶，要注意駭客散佈一封提供假YouTube Video網址下載影片的電子郵件，這封電子郵件會誘使網友連接含有惡意軟體或木馬程式的網站，必須提高警惕。

SophosLabs指出，駭客組織利用最近當紅的YouTube數位影片分享網站，大量寄發標題爲「Dudeyour gonna get caught，lol」、「LOL，dude

廣告

無法顯示網頁

目前查閱的網頁無法使用。網站可能發生技術問題

請嘗試下列:

- 請按 [重新整理] 按鈕，或者稍後再試一次
- 如果在網址列輸入網址，請確定未拼錯任何
- 要檢查您的連線設定，請按[工具]功能表，
項]。在[連線]標籤按[區域網路設定]。
(LAN) 系統管理員或網際網路服務提供者
- 要檢視您的網際網路連線設定值是否正被偵

2015釣魚類型

課程綱要

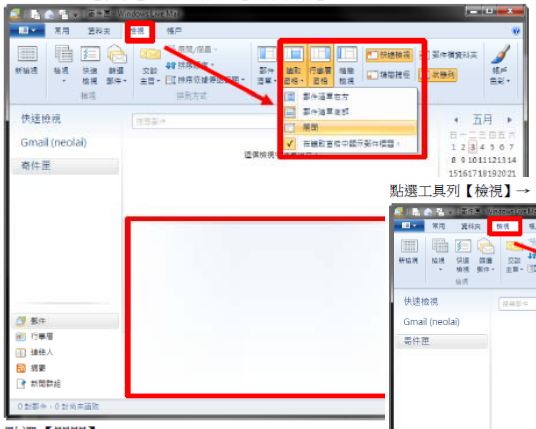
- 電子郵件安全管理

關閉信件預覽功能 Windows

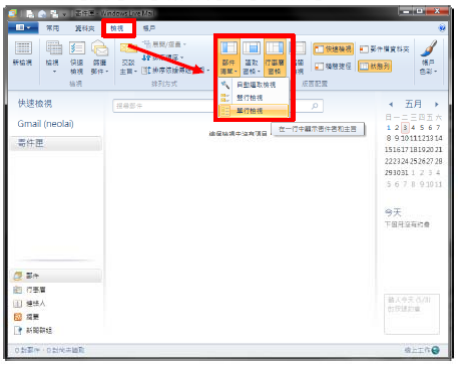
- Windows Live Mail
  - 選取【檢視】/【版面配置】
  - 不勾選【顯示預覽窗格】
- Outlook express
  - 選取【檢視】/【版面配置】
  - 不勾選【顯示預覽窗格】
- Outlook 2010
  - 選取【檢視】 /【讀取窗格】
  - 選擇【關閉】
- Outlook 2007
  - 選取【檢視】 /【讀取窗格】
  - 選擇【關閉】

關閉信件預覽功能Windows Live Mail

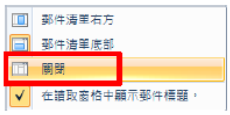
點選工具列【檢視】→版面配置【讀取窗格】。



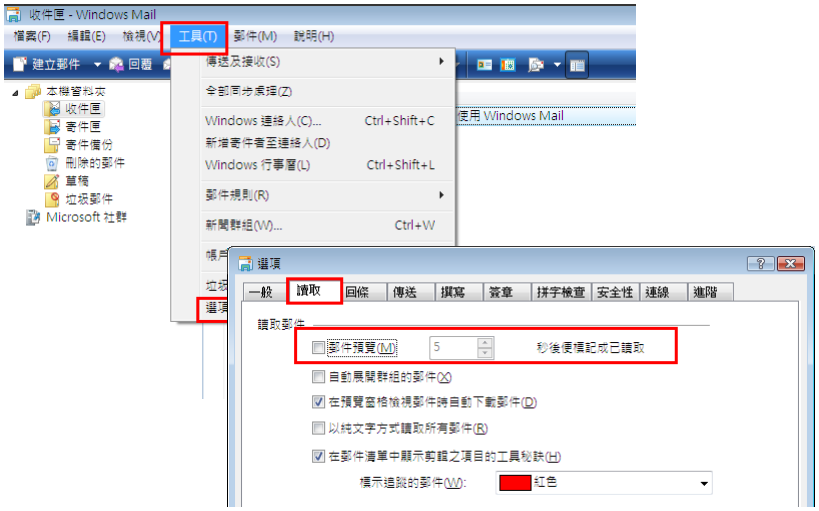
點選工具列【檢視】→【郵件清單】→【單行顯示】。

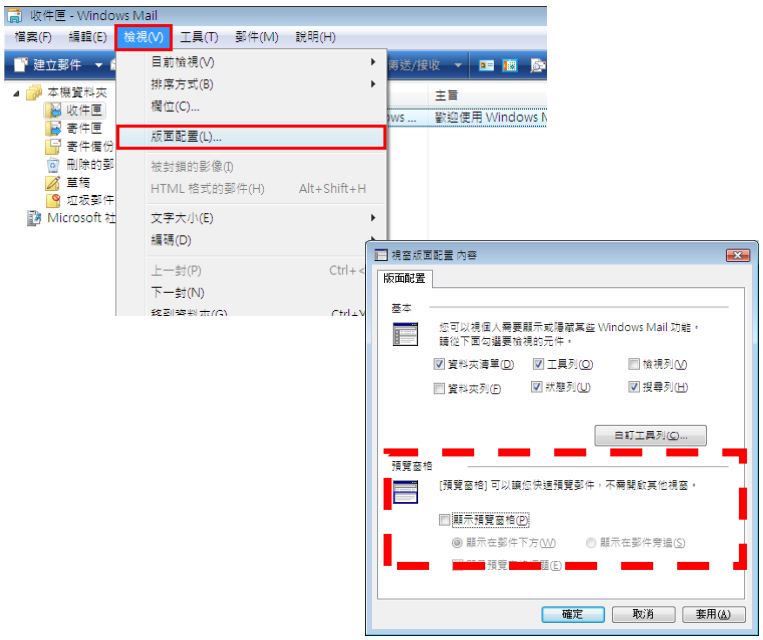


點選【關閉】。

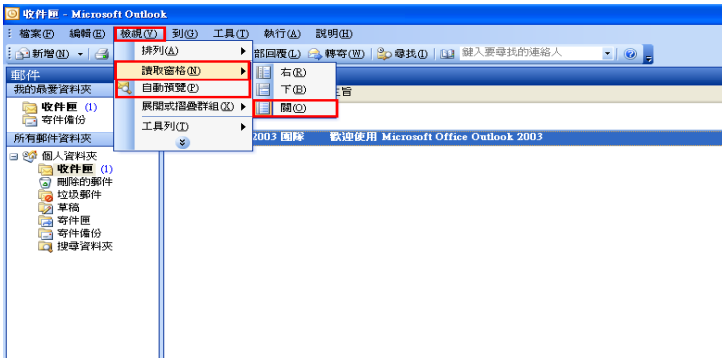


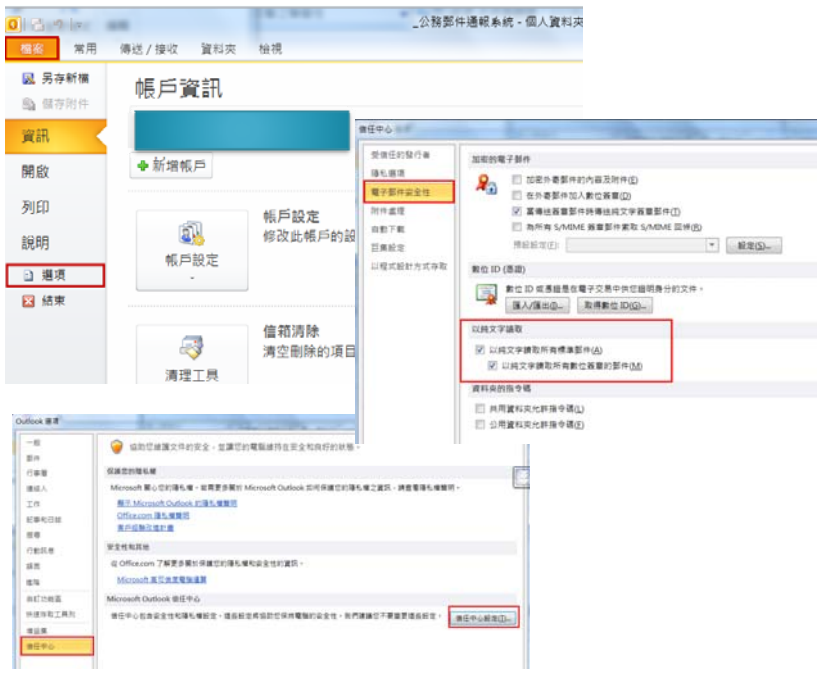
關閉信件預覽功能outlook-express





關閉信件預覽功能outlook





關閉信件預覽功能WEB版

- 【信件預覽功能】：請設定為「**隱藏**」。
- 【阻擋HTML電子郵件中的圖片和其他內容】：請設定為「**啟用**」。
- 【啟用純文字內容顯示】：請設定為「**啟用**」。
- 「**儲存**」按鈕

關閉信件預覽功能智慧型手機

iPhone 關閉郵件預覽功能

關閉信件預覽功能智慧型手機(續)

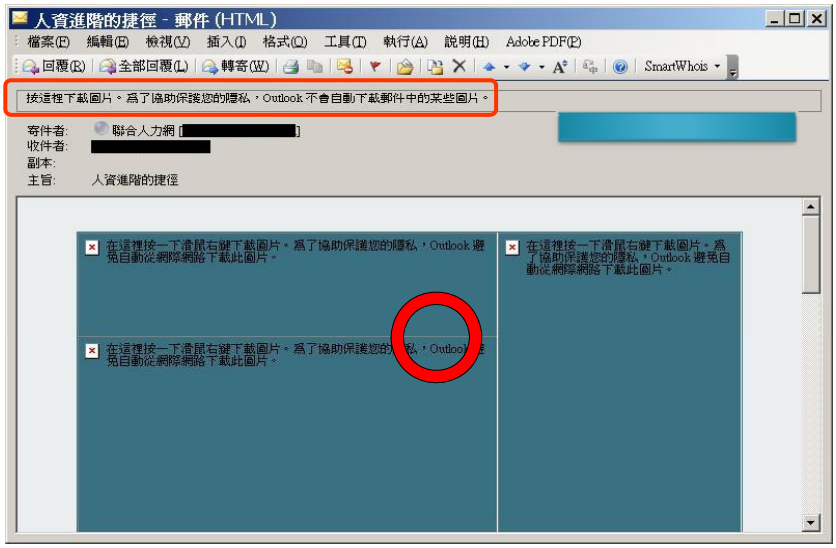
Android關閉郵件預覽功能

關閉自動下載圖檔

- Windows Live Mail
  - 選取【工具】/【安全性選項】/【安全性】
  - 勾選【阻擋HTML電子郵件中的圖片和其他外部內容】
- Outlook express
  - 選取【工具】/【選項】/【安全性】
  - 勾選【阻擋HTML電子郵件中的圖片和其他外部內容】
- Outlook 2010
  - 選取【檔案】/【選項】/【信任中心】/【信任中心設定】/【自動下載】
  - 勾選【不自動下載HTML電子郵件訊息或RSS項目中的圖片】
- Outlook 2007
  - 選取【工具】/【信任中心】/【信任中心設定】/【自動下載】
  - 勾選【不自動下載HTML電子郵件訊息或RSS項目中的圖片】

關閉郵件自動下載圖片及其他內容

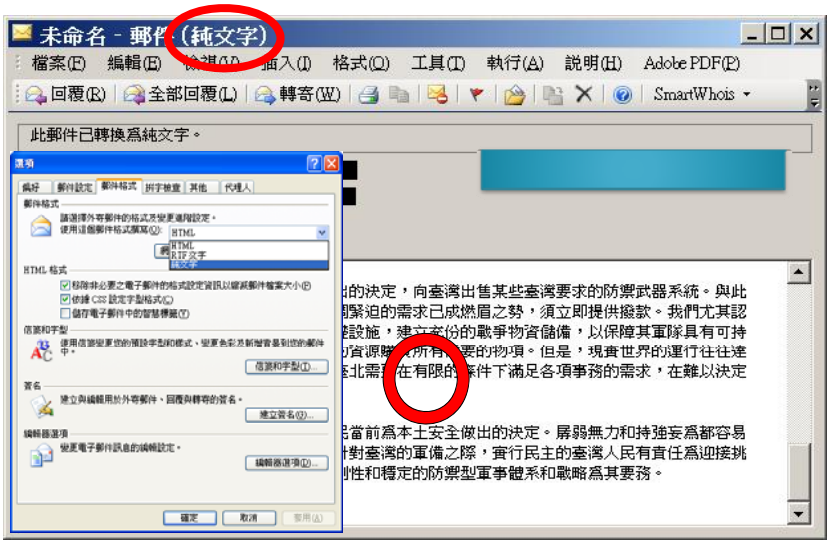
關閉郵件自動下載圖片及其他內容(續)



以純文字開啟信件

- Windows Live Mail
  - 選取【工具】/【選項】/【讀取】
  - 勾選【在純文字中讀取所有郵件】
- Outlook express
  - 選取【工具】/【選項】/【讀取】
  - 勾選【在純文字中讀取所有郵件】
- Outlook 2010
  - 選取【檔案】/【選項】/【信任中心】/【信任中心設定】/【電子郵件安全性】
  - 勾選【以純文字讀取所有標準郵件】
- Outlook 2007
  - 選取【工具】/【信任中心】/【電子郵件安全性】
  - 勾選【以純文字讀取所有標準郵件】

以純文字模式開啟郵件



課程綱要

- 有效防護實作討論

讀取信件要領

先確認寄件者
- 是否為您認識的人或業務需要。

確認郵件主旨
- 是否為奇怪的主旨, 或與寄件者不搭的主旨。

- 確定郵件內容是否與寄件者或主旨有關
- 確定郵件內容是否得宜
  - 例如是否得提供個資料機敏資料。
- 是否非得開啟附件或點選連結
- 是否須向寄件者確認

使用者防護停看聽

- **停 – 使用任何電子郵件軟體前，必須先確認**
  - 執行各種作業系統、應用軟體設定更新
  - 必須安裝防毒軟體，並確實更新病毒碼
  - 收信軟體安全性設定
    - 必須以純文字模式開啟郵件
    - 必須取消郵件預覽功能
  - 防止垃圾郵件
    - 設定過濾垃圾郵件機制
  - 啟用個人防火牆

使用者防護停看聽(續)

看 – 開啟電子郵件前應先依序檢視：

【寄件者】:

- 若【寄件者】與您業務相關且認識，並確認電子郵件信箱位址無誤，如有冒用偽裝情形，則建議直接刪除該郵件。

【郵件主旨】:

- 若【郵件主旨】與您業務無關或主旨怪異，則建議直接刪除該郵件。

使用者防護停看聽(續)

聽 – 若懷疑郵件來源，必須進行確認

- 透過電話或電子郵件向寄件人確認郵件真偽

不要在開啟郵件狀況下，直接按刪除鈕，
應回到郵件清單(index)下刪除郵件，
以免無意間直接開啟下一封郵件。

使用電子郵件時應有的習慣

收信

- 檢查寄件者的真偽
- 確認信件內容的真實度
- 不輕易開啟郵件中的超連結以及附件
- 開啟超連結或檔案前，確認對應軟體（如IE、 Office、壓縮軟體）都保持在最新的修補狀態。

轉信或寄信

- 未經查證之訊息，不要轉寄
- 轉寄郵件前先將他人郵件地址刪除，避免別人郵件地址傳出。
- 寄送信件給群體收件者時，應將收件者列在密件副本，以免收件人資訊外洩。

附加檔案

- 若【附加檔案】名稱顯示與您業務無關或檔名怪異、錯誤，請勿開啟【附加檔案】或建議直接刪除該郵件。
- 若有需要開啟【附加檔案】，不得直接點選開啟檔案，應先另存新檔後，再使用相關軟體開啟。