基隆市政府惡意社交工程電子郵件防範措施

一、惡意社交工程電子郵件攻擊

是一種利用人性弱點、人際交往或互動特性發展出來的電子郵件攻擊，被利用來竊取個人或公務資料、機密等。常見手法如下：

（一）假冒寄件者。

（二）與業務相關或令人感興趣的主題、內容。

（三）含有惡意程式的圖片、附件或連結。

二、防範措施

（一）公務電子郵件信箱請勿用於非公務用途，或隨意公開。

（二）應在安全的環境（如安裝防毒軟體並更新病毒碼的公務電腦）收發公務電子郵件。

（三）郵件軟體請進行安全性設定（如以純文字模式開啟郵件或不自動下載圖片等），並取消郵件預覽功能。

（四）收信時請注意郵件之寄件者、主旨與發信時間及內容等是否有異常之處，與本身業務無關或奇怪郵件勿任意開啟，未確認安全性或非必要時請勿開啟附件檔案、點擊連結網址或下載圖片。

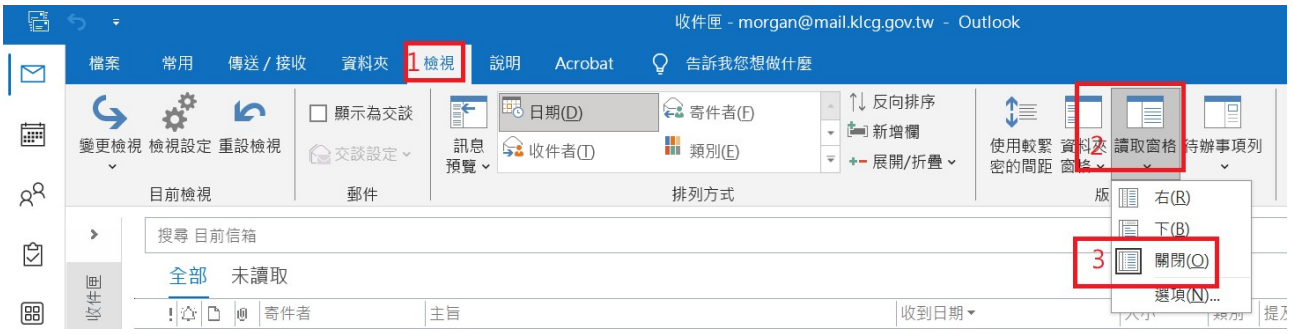
（五）認識的寄信者亦有遭偽冒可能，信件如有可疑時應透過正式、公開或私人管道（如官方網站、電話等）進行查證。

郵件軟體安全性設定教學

本府員工入口網 Web Mail　開啟社交工程防禦

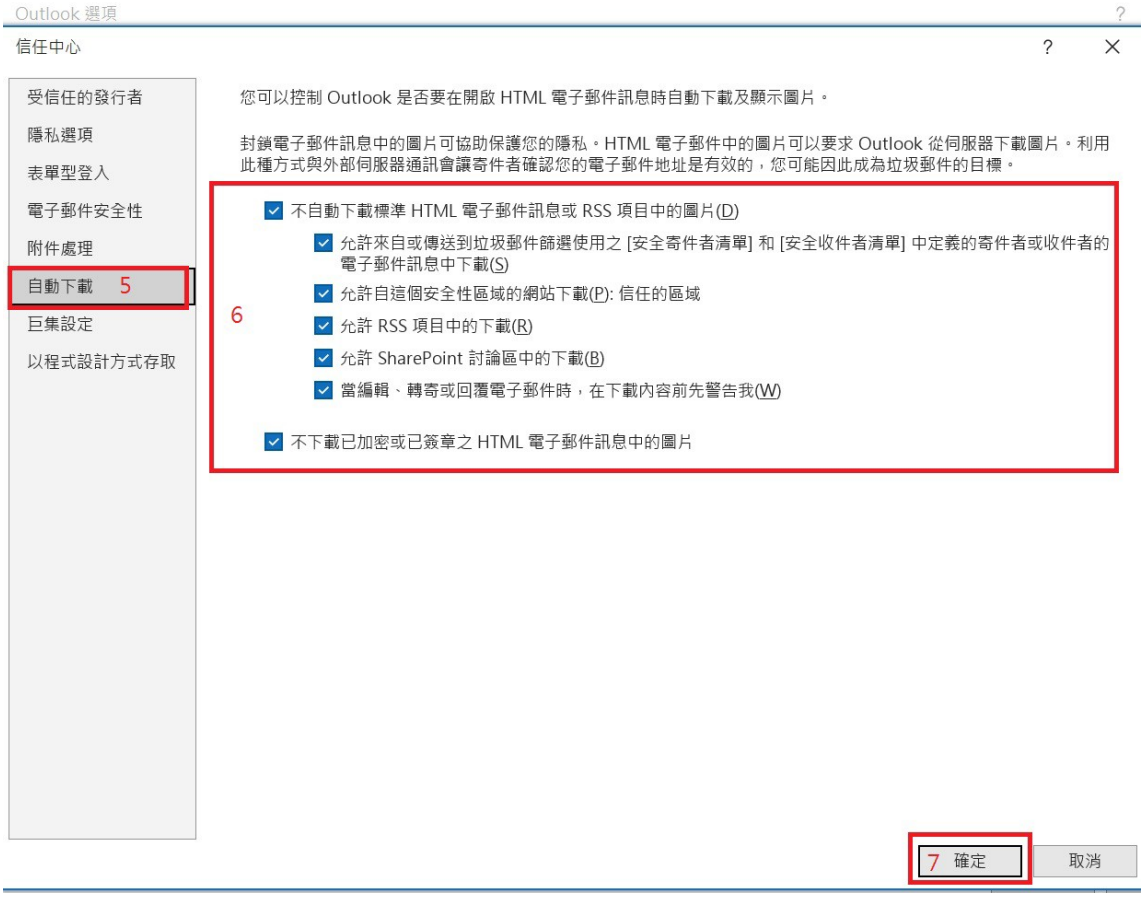
Outlook（以2021為例）

1. 關閉郵件預覽



2. 關閉自動開啟外部圖片


Outlook 選項
一般
郵件
行事曆
人員
工作
搜尋
語言
協助工具
進階
自訂功能區
快速存取工具列
增益集
信任中心 3
協助您維護文件的安全，並讓您的電腦維持在安全和良好的狀態。
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安全性的資訊。
Microsoft 信任中心
Microsoft Outlook 信任中心
信任中心包含安全性和隱私權設定。這些設定將協助您保持電腦的安全性。我們建議您不要變更這些設定。
4 信任中心設定(T)...


Outlook 選項
信任中心
受信任的發行者
隱私選項
表單型登入
電子郵件安全性
附件處理
自動下載 5
巨集設定
以程式設計方式存取
您可以控制 Outlook 是否要在開啟 HTML 電子郵件訊息時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 電子郵件中的圖片可以要求 Outlook 從伺服器下載圖片。利用此種方式與外部伺服器通訊會讓寄件者確認您的電子郵件地址是有效的，您可能因此成為垃圾郵件的目標。
6
不自動下載標準 HTML 電子郵件訊息或 RSS 項目中的圖片(D)
允許來自或傳送到垃圾郵件篩選使用之 [安全寄件者清單] 和 [安全收件者清單] 中定義的寄件者或收件者的電子郵件訊息中下載(S)
允許自這個安全性區域的網站下載(P): 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)
當編輯、轉寄或回覆電子郵件時，在下載內容前先警告我(W)
不下載已加密或已簽章之 HTML 電子郵件訊息中的圖片
7 確定
取消