

資安宣導

社交工程防護

大綱

- 一、社交工程簡介
- 二、常見的社交工程攻擊方式
- 三、防禦方法
- 四、參考資料

大綱

- 一、社交工程簡介
- 二、常見的社交工程攻擊方式
- 三、防禦方法
- 四、參考資料

一、社交工程簡介

- 所謂社交工程，是利用人性方面的各項特性，如：**好奇心**、**同情心**等心理狀態，並利用各種手段讓使用者「**信任**」來進行一種類似「**詐欺**」的攻擊行為，凡是有牽扯到人類因素的任何攻擊行為，都可稱為社交工程。

一、社交工程簡介

常應用之題材

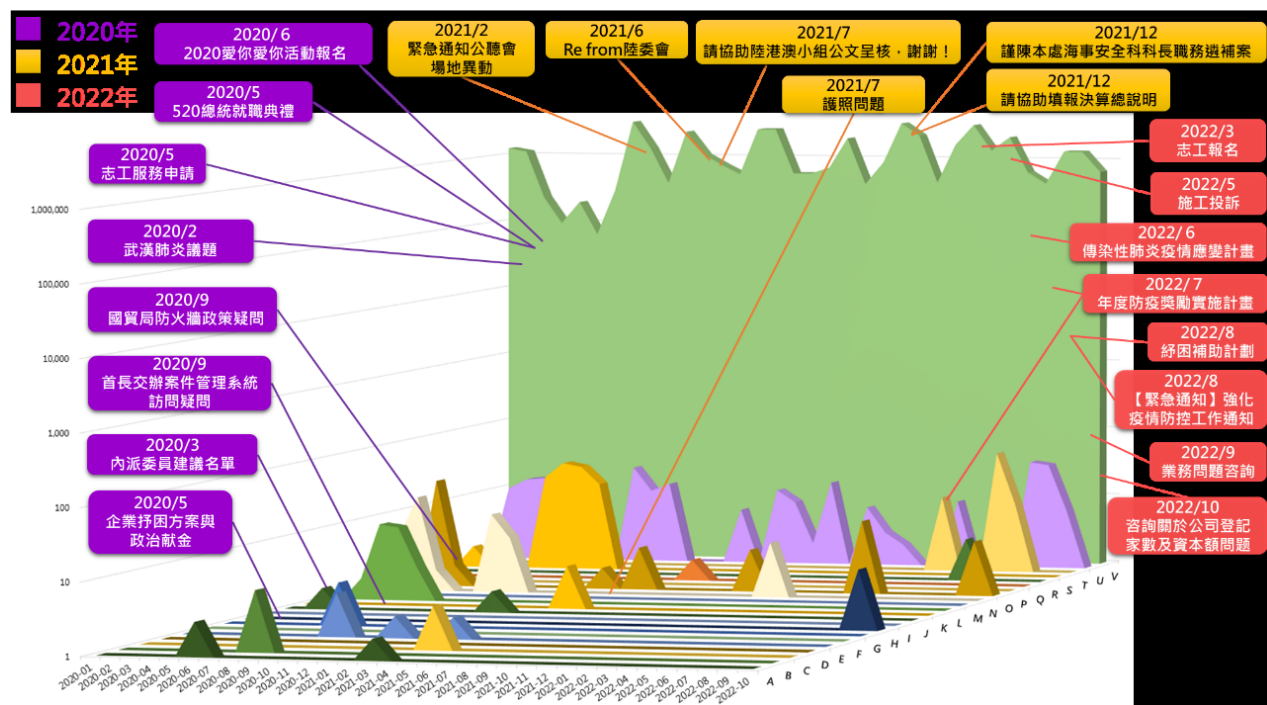
- **重大議題**：您有疫情補貼金可申領！
- **政治**：爆料○長候選人○○○內幕！
- **情色**：藝人○○○手機照片流出！
- **贈品抽獎**：投票抽豪華湯屋雙人券！

大綱

- 一、社交工程簡介
- 二、常見的社交工程攻擊方式
- 三、防禦方法
- 四、參考資料

二、常見的社交工程攻擊方式

- 111年政府領域APT惡意電子郵件攻擊，駭客持續寄送含惡意附檔之電子郵件，以**新冠疫情**、**業務諮詢**等郵件主旨，對政府機關發動魚叉式社交工程郵件攻擊



二、常見的社交工程攻擊方式

➤ 假冒各種身分使你透露出許多重要資訊！



大綱

- 一、社交工程簡介
- 二、常見的社交工程攻擊方式
- 三、防禦方法
- 四、參考資料

三、防禦方法

關閉郵件預覽功能

The screenshot shows the Microsoft Outlook interface with several red boxes and numbered annotations indicating the steps to disable mail preview:

- 1. 選取要修改的資料夾**: A red box highlights the "收件匣 57" (Inbox 57) in the left sidebar.
- 2. 選取上方工具列的「檢視」**: A red box highlights the "檢視" (View) tab in the top ribbon.
- 3. 選取「讀取窗格」**: A red box highlights the "讀取窗格" (Reading Pane) button in the top ribbon.
- 4. 選取「關閉」**: A red box highlights the "關閉" (Close) button in the dropdown menu of the "讀取窗格" button.

The interface also shows a list of emails in the center pane, including one from "Microsoft Outlook" and another from "吳宗鴻".

三、防禦方法

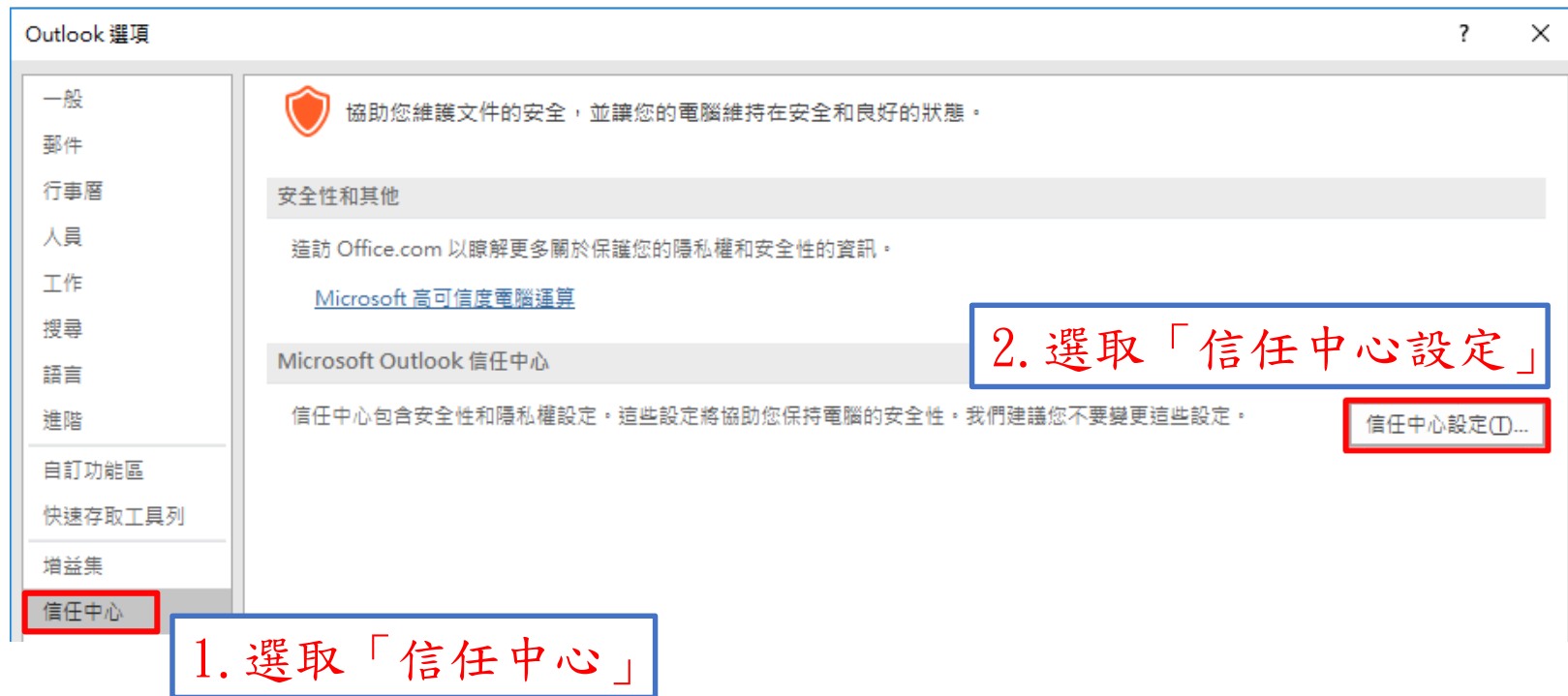
使用純文字模式讀取信件(1/3)

- 因為大多數電子郵件嵌入的惡意程式碼是以html方式撰寫，故使用純文字模式開啟郵件並瀏覽時，並不會主動執行或是下載這些可疑的外部內容。



三、防禦方法

使用純文字模式讀取信件(2/3)



三、防禦方法

使用純文字模式讀取信件(3/3)

The screenshot displays the Outlook 'Trust Center' settings window, specifically the 'Security' tab. The window is divided into two panes. The left pane, titled '信任中心' (Trust Center), lists various security settings. The right pane, titled '電子郵件安全性' (Email Security), contains options for handling email content. Red boxes and numbered text overlays indicate the following steps:

1. 選取「自動下載」 (Select 'Automatic download'). This points to the '自動下載' (Automatic download) option in the '附件處理' (Attachment handling) section of the left pane.
2. 勾選「不自動下載HTML電子郵件訊息或RSS選項中的圖片」 (Check 'Do not automatically download HTML email messages or images in RSS feeds'). This points to the checkbox in the right pane.
3. 選取「電子郵件安全性」 (Select 'Email Security'). This points to the '電子郵件安全性' (Email Security) tab in the right pane.
4. 勾選「以純文字讀取所有標準郵件」 (Check 'Read all standard mail in plain text'). This points to the checkbox in the '以純文字讀取' (Read in plain text) section of the right pane.
5. 點擊「確定」 (Click 'OK'). This points to the '確定' (OK) button at the bottom right of the window.

三、防禦方法

個人平常防禦行為

- 定期更新作業系統與最新修補程式
- 更新防毒軟體病毒碼並定期掃描電腦
- 公務電腦應避免從事非公務之用途
- 不安裝來路不明的應用程式
- 不開啟來路不明的電子郵件及附加檔案
- 不開啟及登入未經確認的網站

大綱

- 一、社交工程簡介
- 二、常見的社交工程攻擊方式
- 三、防禦方法
- 四、參考資料

四、參考資料

- 行政院國家資通安全會報技術服務中心111年第2次政府資通安全防護巡迴研討會政府機關資安威脅與防護重點

感謝閱讀