教育部114年防範惡意電子郵件社交工程演練宣導

國立臺南大學圖資處

114年3月

教育部114年社交工程演練計畫

- 對象：人員範圍為學校全體人員（定義為具備公務電子郵件帳號者），不限於正式公務人員身分。(本校提報參與演練人員467人)
- 演練時程：自114年4月至12月止，期間辦理2次演練。
- **社交工程演練郵件型態：**以偽冒公務、個人或公司行號等名義，發送社 交工程演練郵件 交工程演練郵件 給受測人員 ，郵件主題分為八卦、休閒、保健、財經、新奇、時事、模擬實際社交工程樣本等類型，郵件內容包含連結網址或附檔。

教育部演練目的

- 社交工程為駭客常用入侵管道，**透過電子郵件夾帶惡意程式或連結網址等方式**，輔以吸引人之信件主旨及內容，誘使缺乏警戒心的使用者開啟後造成進一步破壞，且多有實際入侵成功案例，嚴重損害機關或個人之權益。

- 為依資通安全法令規定及增進臺灣學術網路安全之目的，持續辦理本(113)年度本部、所屬公務機關及臺灣學術網路之社交工程演練服務，並訂定本計畫，透過實施演練作業，**提升教育體系人員針對社交工程攻擊之警覺性**，並檢驗機關防範社交工程成效，及透過後續持續改善降低社交工程風險。

教育部113年第2次防範惡意電子郵件社交工程演練信件標題

類別	信件標題
擬真類	「全透明文字」一招讓iPhone鎖定畫面變高級！隱私不外漏
公務類	行政院拍板　軍公教明年調漲薪資
情色類	震撼宣布下海！40路陳沂「開戰前倒奶預告」
旅遊類	【台東熱汽球嘉年華攻略】三麗鷗聯名、光雕音樂會亮點一次看！
旅遊類	旅遊補助加碼，跟團自由行都有！符合條件領1000元

教育部113年第1次防範惡意電子郵件社交工程演練信件標題

類別	信件標題
美容類	吃保健品美膚？營養師：搞懂5成分 免花冤枉錢
科技類	iPhone用戶注意！新病毒「盜銀行資料」受害者集中亞洲
時事類	電信防堵詐騙語音上線！聽到「這14字」考慮過後再接
旅遊類	北港糖廠鐵道地景文化空間完工 打造不一樣的糖廠風貌
擬真類	超商禮券1000元序號通知(請於1小時內領取)

教育部112年第1次防範惡意電子郵件社交工程演練信件標題

類別	信件標題
公務類	您已接受邀請共用此行事曆
科技類	ChatGPT官方APP來了！台灣開放下載 iPhone搶先試
情色類	補教狼師MeToo！最美禮生控「18歲生日遭揉胸強吻」
休閒類	連假這樣請半個月都不用上班！快訂機票半月遊！
財經類	夏季電費6月上路！台電估計約378萬戶不漲價，原因曝光

教育部112年第2次防範惡意電子郵件社交工程演練信件標題

類別	信件標題
科技類	微軟也計畫將人工智慧應用至OneDrive雲端儲存服務
保健類	肺炎鏈球菌疫苗將放寬65歲以上免費接種！5種接種建議
生活類	嚇阻酒駕、肇逃！ 短期駕照最快明年3月上路
旅遊類	日本環球影城 遊阪必到超夯樂園嗨翻玩
時事類	不只郭賴配？中選會公告10組正副總統候選人！

電子郵件社交工程攻擊

何謂社交工程

利用人性弱點,
應用簡單的溝通
和欺騙技倆。

獲取帳號、
密碼、
身分證號碼或
其他機敏資料。

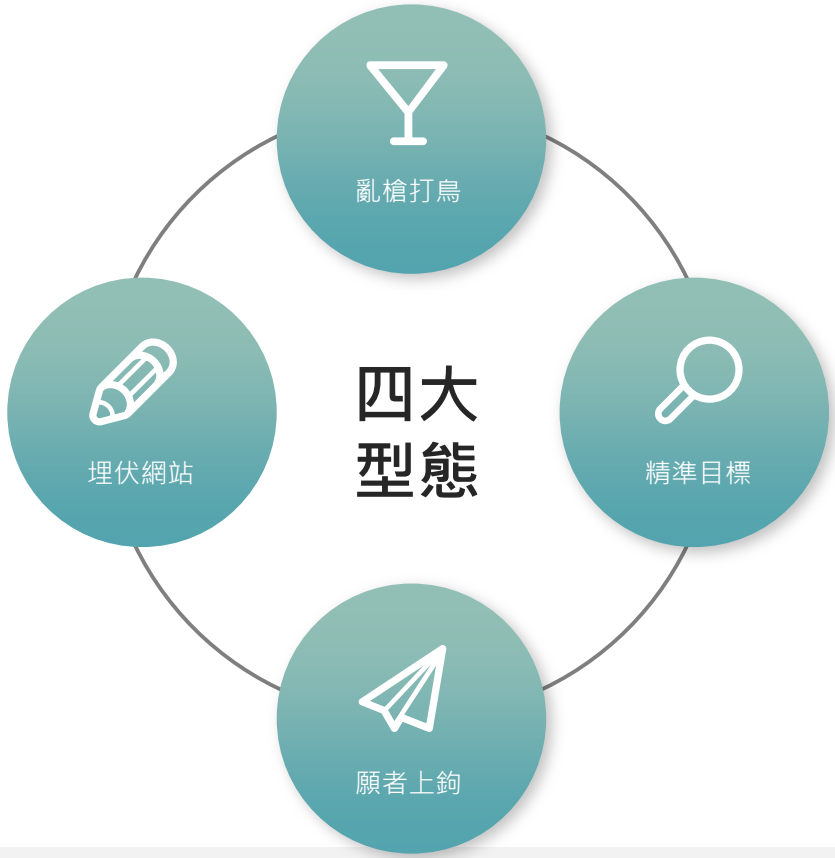
突破企業的
資通安全防護

行非法的存取、
破壞行為

社交工程攻擊目的


竊取
機密檔案
及文件
蒐集
針對性
資料
蒐集
使用者
個人資料
竊取
部落格或
社群網站之
帳號密碼
目的
竊取
商業機密
資料
監控
使用者行為
竊取
網路服務之
有價財產
成為跳板、
殭屍電腦

常見的社交工程攻擊型態



亂槍打鳥--垃圾誘餌攻擊

根據社會時事，攻擊者寄送惡意程式郵件或訊息。這些資料訊息的標題通常包含「吸引人」的社會事件。

精準目標--魚叉式攻擊

針對特定目標或特定機構的員工，觀察其社群媒體帳號，精心製作出很有說服力的手機訊息或電子郵件內容，並且挾帶可造成感染的附件檔或URL連結。

埋伏網站--水坑式攻擊

先觀察目標習慣瀏覽哪一些網站？接著去入侵網站並植入惡意程式，等待目標對象、造訪網站，再趁機感染惡意程式竊取資料。

願者上鉤--釣魚式攻擊

先製作假網站，攻擊者寄送電子郵件，誘騙受害者到這些假網站。這些假網站通常偽裝成「金融」或是「信箱」的異常通知。

各種社交工程攻擊手法

偽裝維護人員、
上級單位人員，
騙取帳號及密碼。

利用工具軟體、
檔案、圖片誘騙
下載，乘機
植入惡意程式，
暗中收集
機敏性資料。

利用電話
佯裝資訊人員，
騙取帳號及
密碼。

利用電子郵件
誘騙開啟檔案、圖片，以植入惡意程式、暗中收集機敏性資料。

利用電子郵件
誘騙使用者
登入偽裝網站，
騙取帳號及
密碼。

利用通訊軟體，偽裝親友來訊，誘騙點選連結後，植入惡意程式。

社交工程攻擊共同點

資料來源：趨勢科技

強化社交工程郵件防範

國家資通安全研究院
National Institute of Cyber Security

- 避免開啟非公務相關郵件，降低社交工程攻擊威脅
- 應建立電子郵件過濾機制，並加強郵件驗證機制與保留郵件日誌，以利溯源分析，例如密碼暴力破解登入或其他異常活動跡象
- 定期或不定期執行社交工程演練，辦理資安認知教育訓練，強化人員識別與判斷社交工程郵件之能力

確認信件來源

- 確認寄件者、寄件來源IP、附件檔案及信件內容(如網路連結)

設置垃圾郵件過濾設備

- 落實資通安全防護應辦事項，設置電子郵件過濾機制

保護資訊設備安全

- 定期進行系統安全性檢測，注意個別系統之安全修補與病毒碼更新

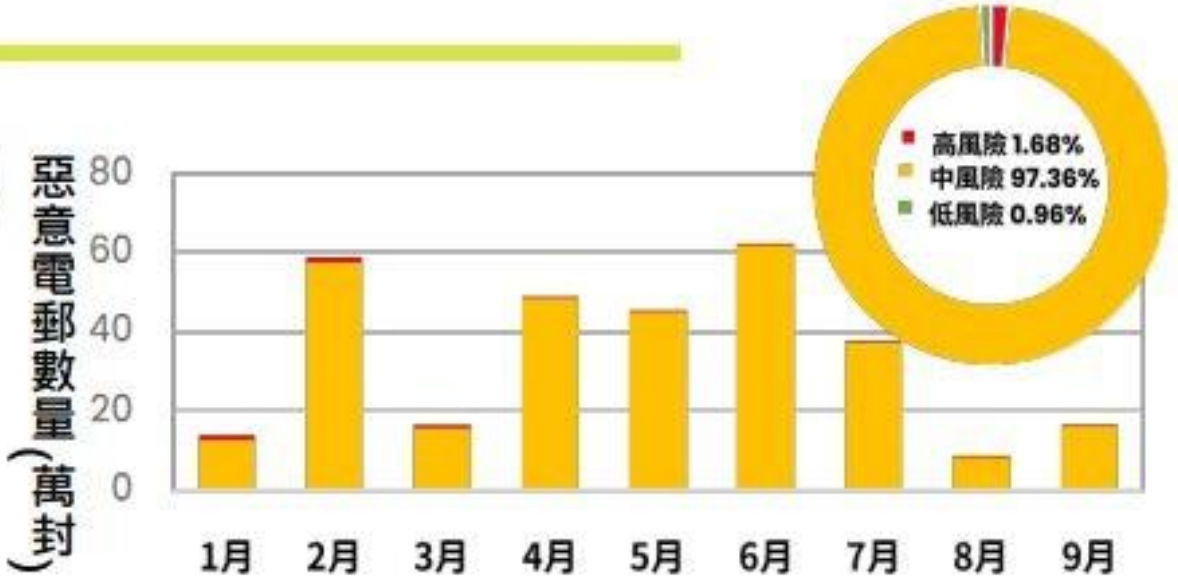
定期演練

- 藉由演練強化人員防護意識

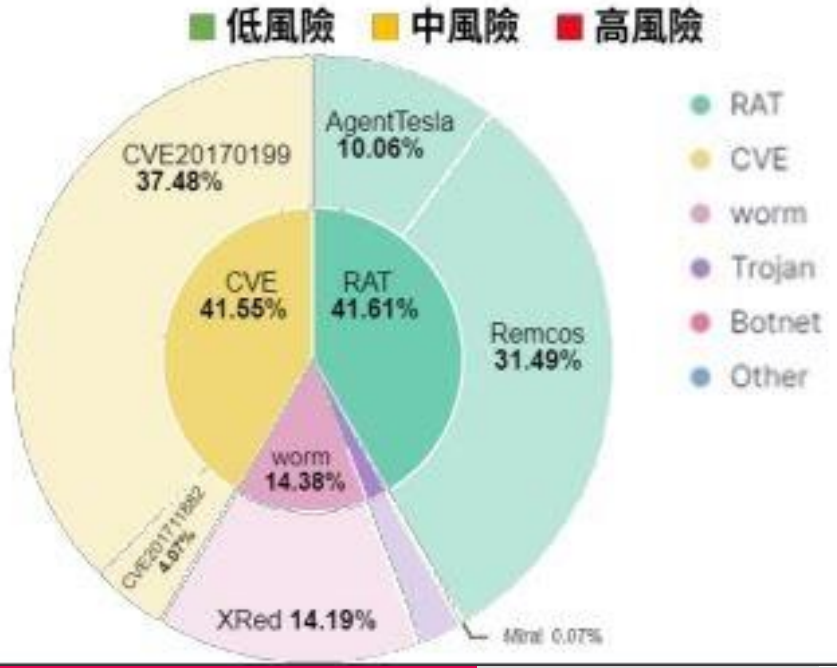
資料來源：國家資通安全研究院

惡意電子郵件分析

- 113年共檢測1.6億餘(166,215,880)封電子郵件，偵測發現**308萬餘(3,080,336)封可疑惡意電子郵件**，占1.85%



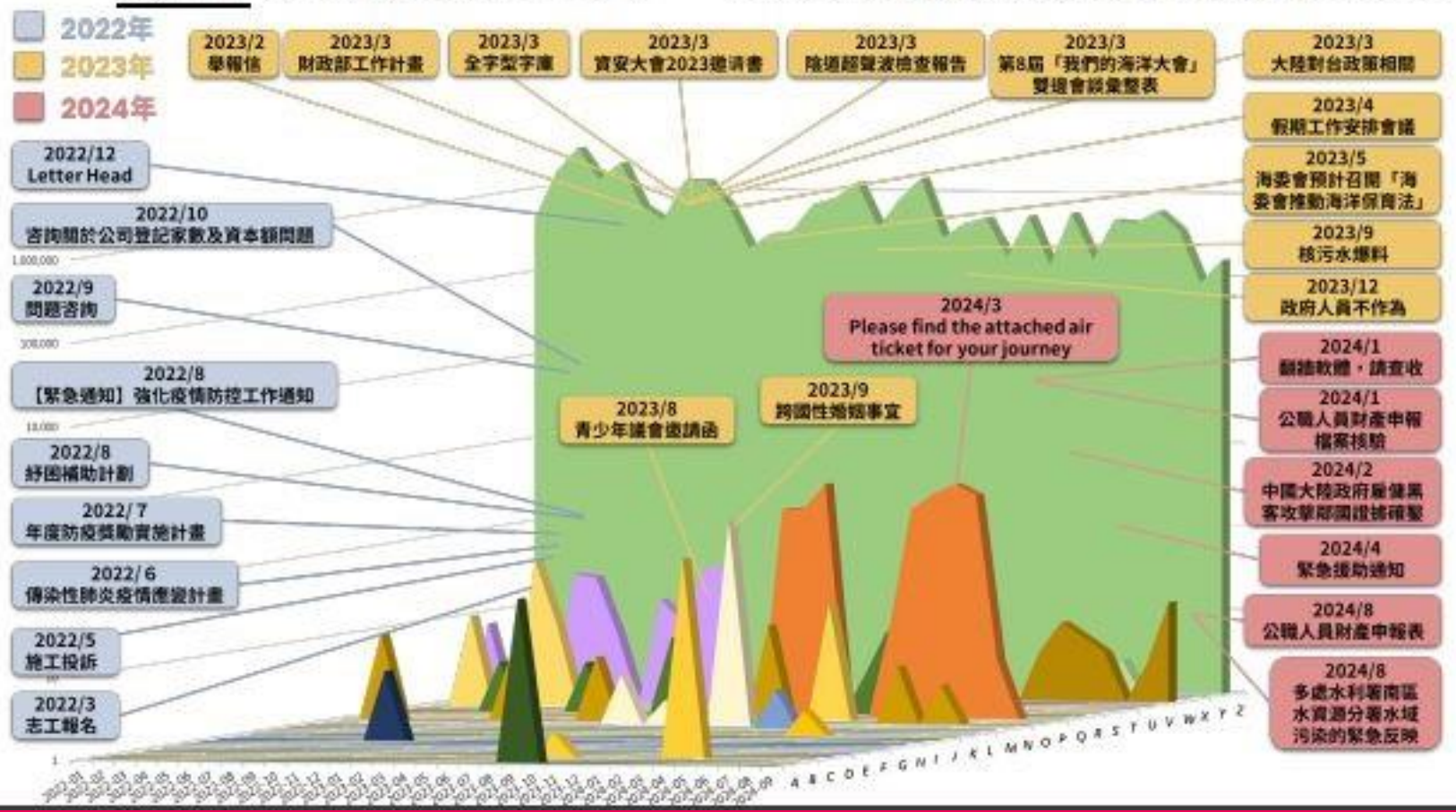
- 含惡意附檔之郵件中，以散布**CVE-2017-0199**漏洞利用之惡意文件最多，其次則為遠端木馬**Remcos**與後門程式**XRed**



惡意電子郵件分析

國家資通安全研究院
National Institute of Cyber Security

- 113年政府領域APT郵件攻擊趨勢可歸納為**7波攻擊行動**，計**608封針對性社交工程郵件**，駭客利用公職人員財產申報、差旅訂票及檢舉爆料等引誘性主旨，對政府機關人員發動攻擊

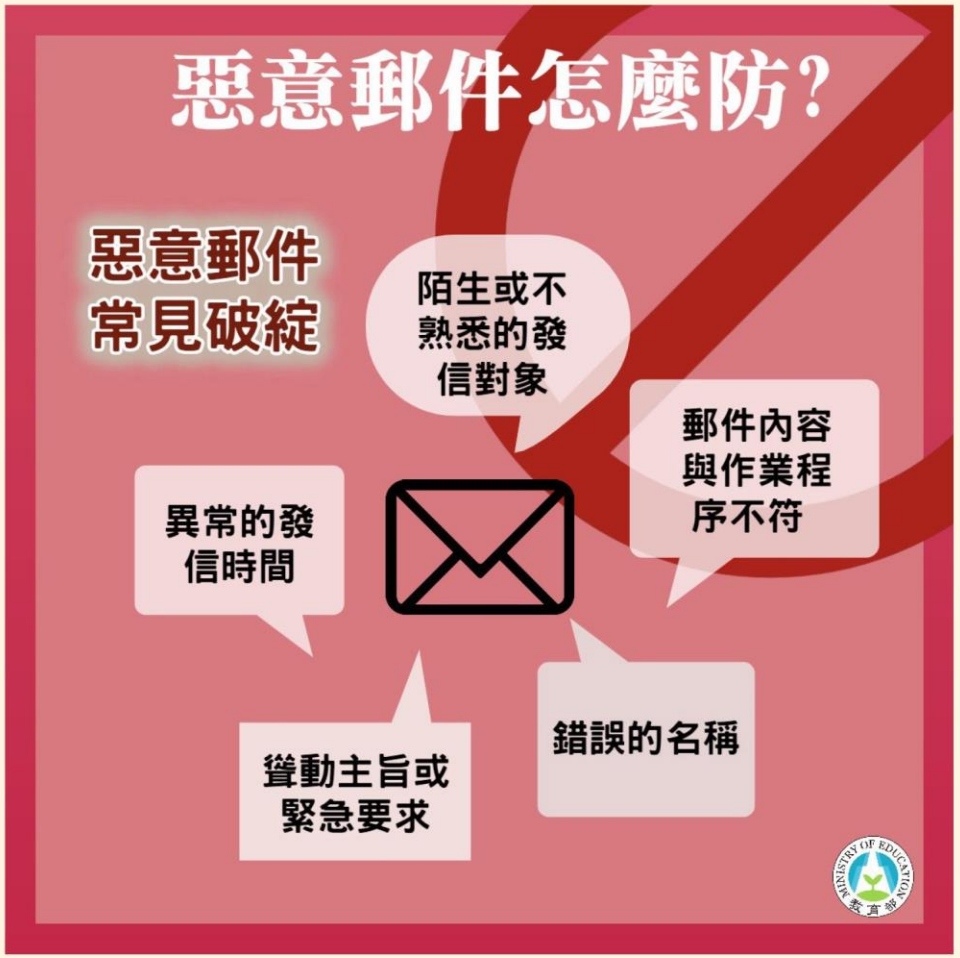


113年APT郵件攻擊手法

- 濫用合法郵件服務與使用者互動之多層式攻擊策略
- 以公職人員財產申報為由散布Star RAT遠端木馬程式
- 利用Office漏洞(CVE-2017-0199)搭配華航訂票相關主旨
- 以水汙染檢舉為由，利用MSC文件之新型態攻擊手法下載Cobalt Strike後門程式

防範電子郵件社交工程攻擊

社交工程攻擊防範


惡意郵件怎麼防?
惡意郵件
常見破綻
陌生或不熟悉的發信對象
郵件內容與作業程序不符
異常的發信時間
錯誤的名稱
聳動主旨或緊急要求

社交工程攻擊防範

防範社交工程停看聽

- 注意陌生或不熟悉的寄件者
- 注意是否與公務有關

社交工程攻擊防範

防範社交工程停看聽

- 寄件人與標題是否正確
- 與本身業務是否相關

不直接開啟

社交工程信件常見破綻

- 錯誤的名稱
- 異常的發信時間
- 郵件內容與作業程序不符
- 聳動或為緊急要求

社交工程攻擊防範

防範社交工程停看聽

- 主動聯繫相關單位確認真偽
- 仍有疑義請洽機關資安窗口

若仍有業務上收信之需求，
可將可疑信件打包匯出後，
寄送資安窗口確認

資安趨勢部落格

https://blog.trendmicro.com.tw/?p=75788

什麼是社交工程(Social Engineering)？該如何保護自己？

2023 年 01 月 05 日　趨勢科技 TrendMicro　熱門推薦, 社交工程 (social engineering) , 資安名詞

社交工程(Social Engineering)是一種攻擊者利用與人互動和操弄來達到目的的技術。通常涉及說服受害者為了攻擊者的金錢或資訊利益而危害自身安全或破壞安全最佳作法。駭客經常會用社交工程來偽裝自己及動機，通常是冒充成可信任的對象。

警政署165全民防騙網—常見詐騙手法宣導

刑事警察局公告高風險業者

統計時間
114.02.08-02.14

遭冒名業者

解除分期付款詐騙
(假冒消費異常詐騙)

無

如接獲以上業者假客服電話、可疑Line客服帳號，除撥打165專線舉報
建請速向業者反映遭詐情事，以維護您的權益!

防詐重點

1、業者及銀行客服絕不會來電要求您操作網路銀行或ATM解除錯誤設定。
2、慎防假買家提供**假客服**連結/QR Code，以認證/簽署○○協定話術要求操作ATM。
3、接獲**帶+號境外**或陌生來電，務必提高警覺。

平臺名稱

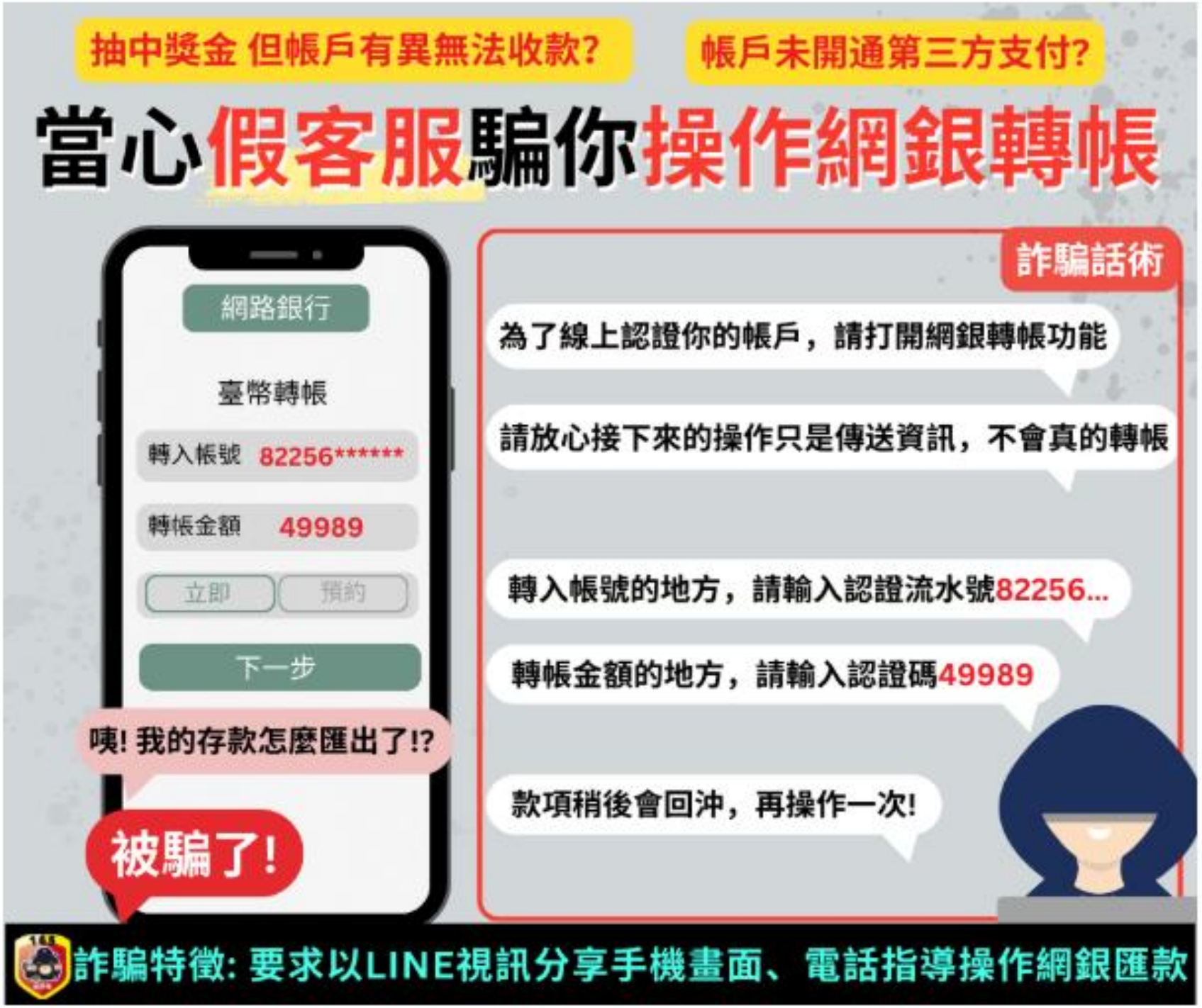
假網拍詐騙

Facebook
LINE社群
Instagram
Threads

防詐重點

FB、LINE、IG沒有安全交易保障機制，**請勿於社群平臺購物**。

請慎選優良有信用，且提供**第三方支付**之網購平臺，保障消費權益。


抽中獎金 但帳戶有異無法收款?
帳戶未開通第三方支付?
當心假客服騙你操作網銀轉帳
網路銀行
臺幣轉帳
轉入帳號 82256******
轉帳金額 49989
立即
預約
下一步
咦! 我的存款怎麼匯出了!?
被騙了!
詐騙話術
為了線上認證你的帳戶，請打開網銀轉帳功能
請放心接下來的操作只是傳送資訊，不會真的轉帳
轉入帳號的地方，請輸入認證流水號82256...
轉帳金額的地方，請輸入認證碼49989
款項稍後會回沖，再操作一次!
詐騙特徵: 要求以LINE視訊分享手機畫面、電話指導操作網銀匯款

內政部警政署165全民防騙網
113/12/9-113/12/15詐騙來電排名

113/12/9-113/12/15詐騙來電排名

發佈日期：2024-12-18 19:18

更新日期：2024-12-20 19:18

詐騙來電排名(統計日期：113年12月9日至113年12月15日)		
1	+18003958423	假借個人資料外洩詐財
2	+18007165686	假借個人資料外洩詐財
3	+85295779671	假網拍
4	+932109917	猜猜我是誰
5	281010700	假網拍
6	+12024026170	色情應召詐財
7	+12027788831	假慈善機關(急難救助)
8	+13058767501	色情應召詐財
9	+13322721532	假冒機構(公務員)詐財
10	+13478328515	猜猜我是誰

國立臺南大學電子郵件社交工程演練資訊網及資通安全宣導網

https://www.nutn.edu.tw/cc/emailse

網路地圖 回到首頁 臺南大學

最新消息 NEWS
網站說明 ABOUT
自我防護 PROTECTION
演練成果 EXHIBITION
相關連結 LINK
網頁地圖 SITEMAP

最新消息 News_event

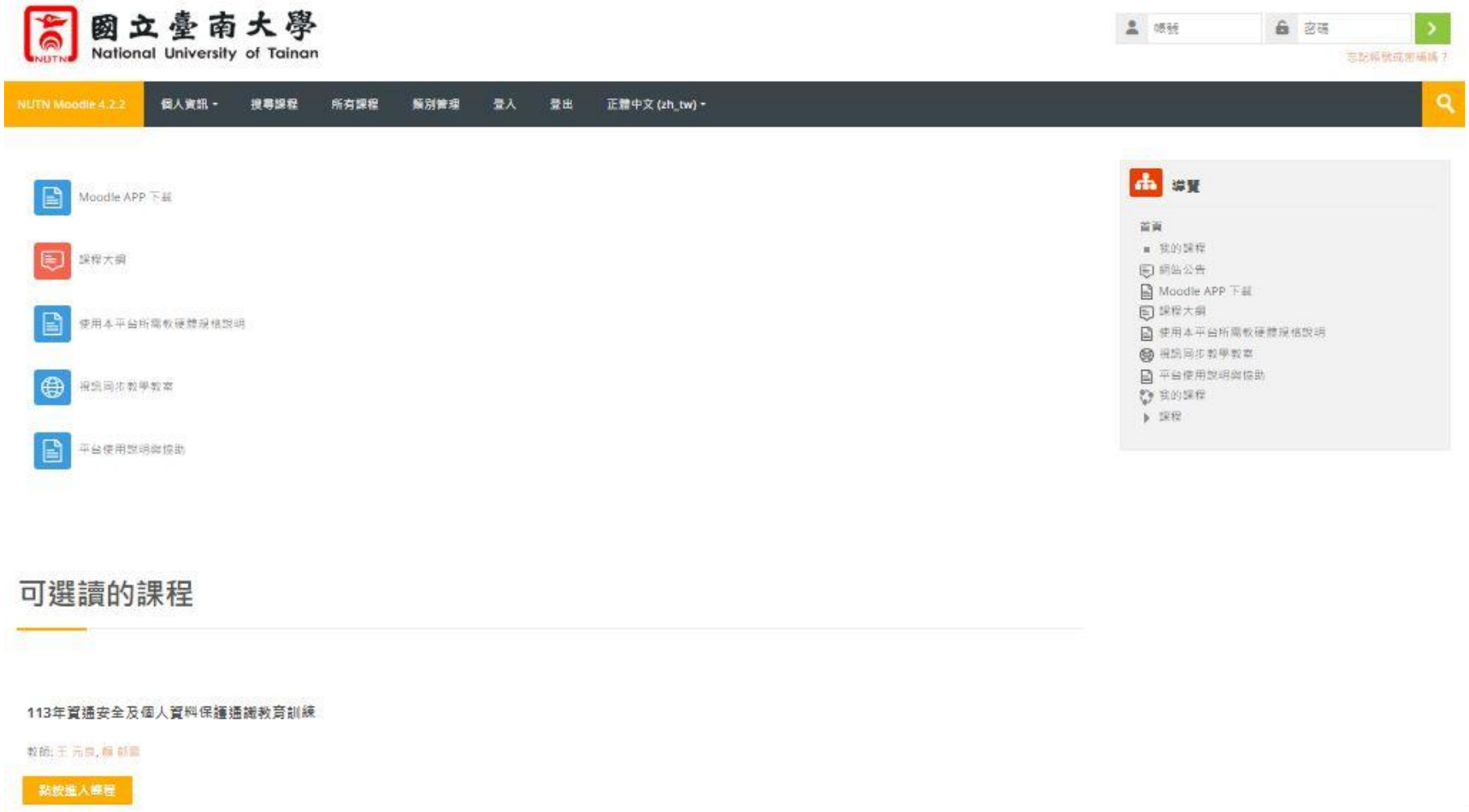
連絡資訊

國立臺南大學圖資處
王元良先生 分機601
yuan@mail.nutn.edu.tw

https://isms.nutn.edu.tw

資通安全及個人資料保護通識教育訓練(含政策宣導)—南大moodle線上課程

https://moodle.nutn.edu.tw/moodle



牛刀小試—
南大防範惡意電子郵件社交工程認知素養線上評量

國立臺南大學社交工程認知素養線上評量

https://forms.gle/s9Nw24vXq9HgZM1u7

國立臺南大學114年防範惡意電子郵件社交工程認知素養線上評量

感謝南大教職員同仁參與評量，共同強化本校人員防範惡意電子郵件社交工程及資安素養。

登入 Google 即可儲存進度。瞭解詳情

* 表示必填問題

單位 *

您的回答

姓名 *

您的回答

感謝師長閱讀與配合
提升防範惡意電子郵件社交工程成效