# 教育部115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

115年3月

本校人員114年第1次「開啟郵件」比率為5%、「點閱連結」及「開啟附件」比率為0%。
第2次「開啟郵件」比率為4%、「點閱連結」及「開啟附件」比率為0%　，**成績符合教育部惡意郵件開啟率應低於10%、點閱率應低於6%以下標準。**

**感謝各單位師長同仁協助與配合。**

# 本校參與教育部114年防範惡意電子郵件社交工程演練結果

# 教育部115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**一、二級主管、教職員及計畫助理**等一般行政人員469人參與演練)
- 演練時程：自115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(115)年度教育部、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115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 |
| --- | --- |
| 擬真類 | 偵測到0utlook連續登入失敗　請重設密碼 |
| 休閒類 | 便宜機票要來了！長榮航總經理：「這航線」降價會很有感 |
| 公務類 | 內部講座活動通知 |
| 情色類 | 超兇畫面晃爆！鏡子出賣「林襄傲人車頭燈」 |
| 財經類 | 黃金大反彈！專家：「這時」將上看5000美元 |

# 教育部115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 |
| --- | --- |
| 休閒類 | 2026年行事曆搶先看！假日多5天「9連假請假攻略必看」 |
| 擬真類 | 【出貨通知】您所訂購的商品已出貨 |
| 公務類 | 【公告】職安宣導：新冠疫情已升溫，其實你可能已中標！ |
| 八卦類 | 人氣更勝李多慧？韓國「啦啦隊女王」廉世彬將來台 |
| 保健類 | 咖啡越喝越累！喝錯時間＝偷走睡眠，醫揭「最佳飲用時段」 |

# 電子郵件社交工程攻擊

# 何謂社交工程

**提醒：**
**寄件者顯示名稱**
**寄件者來源信箱**
**主旨**
**均可偽造**



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

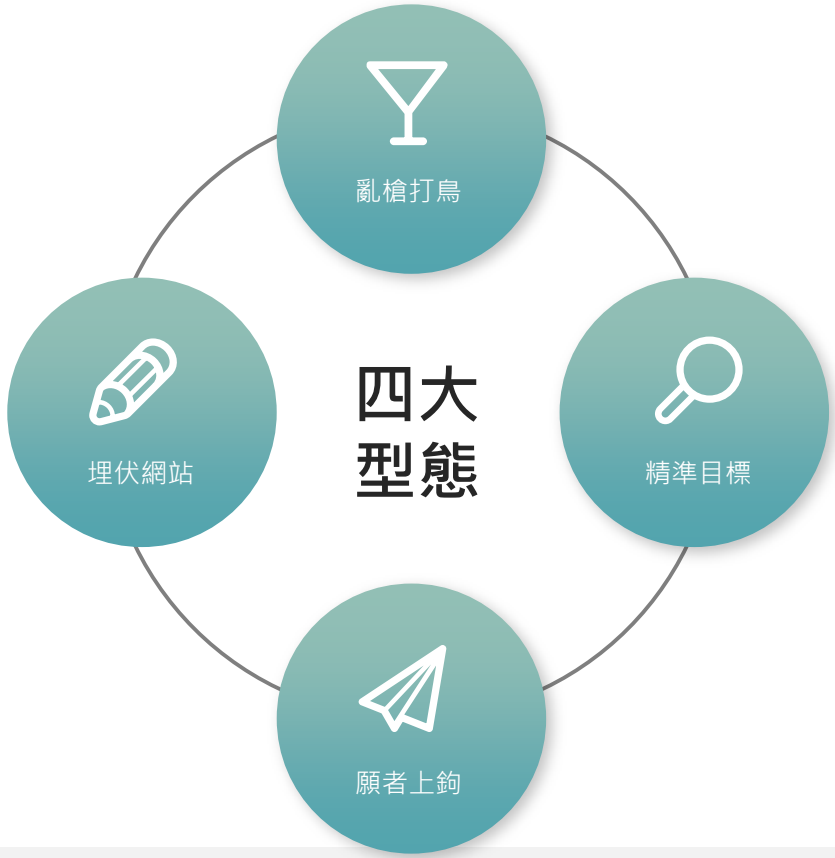


行非法的存取、
破壞行為

# 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。

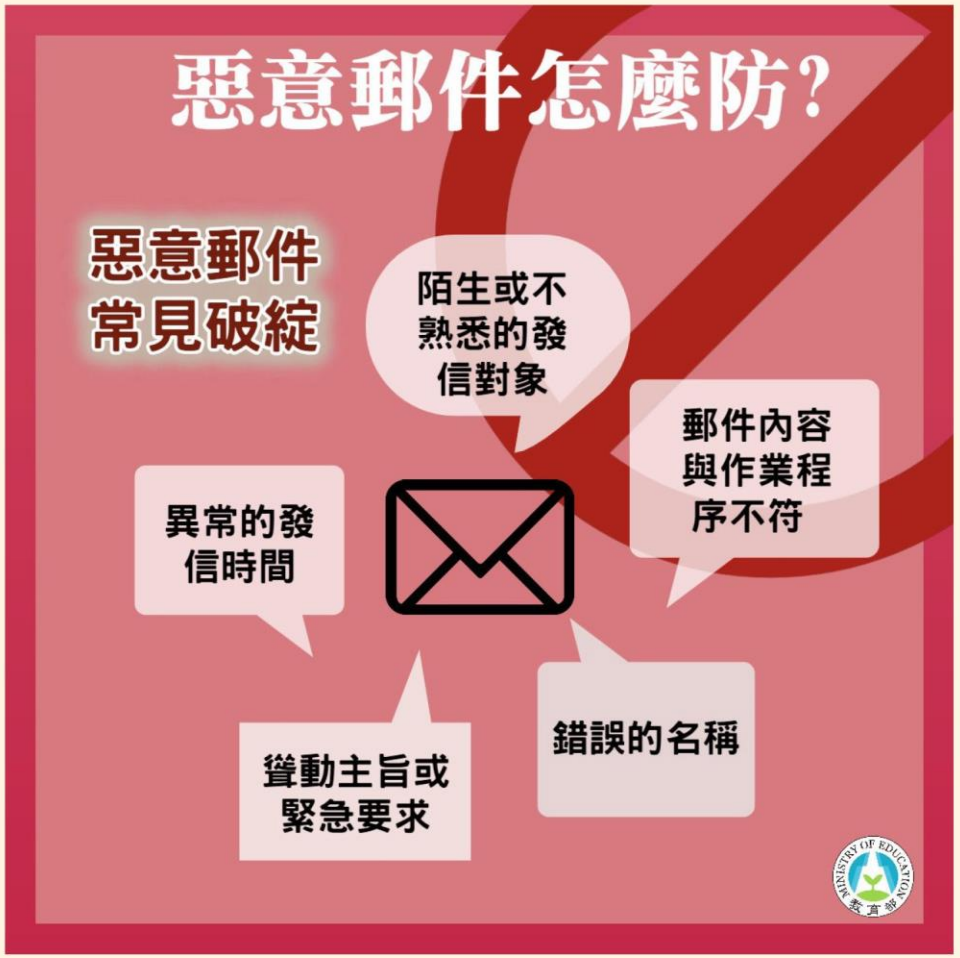
# 社交工程攻擊共同點




資料來源：趨勢科技

# 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
聳動主旨或緊急要求
錯誤的名稱

# 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。

# 資安趨勢部落格

**電子郵件社交工程攻擊之後，運用勒索軟體綁架電腦資料。**



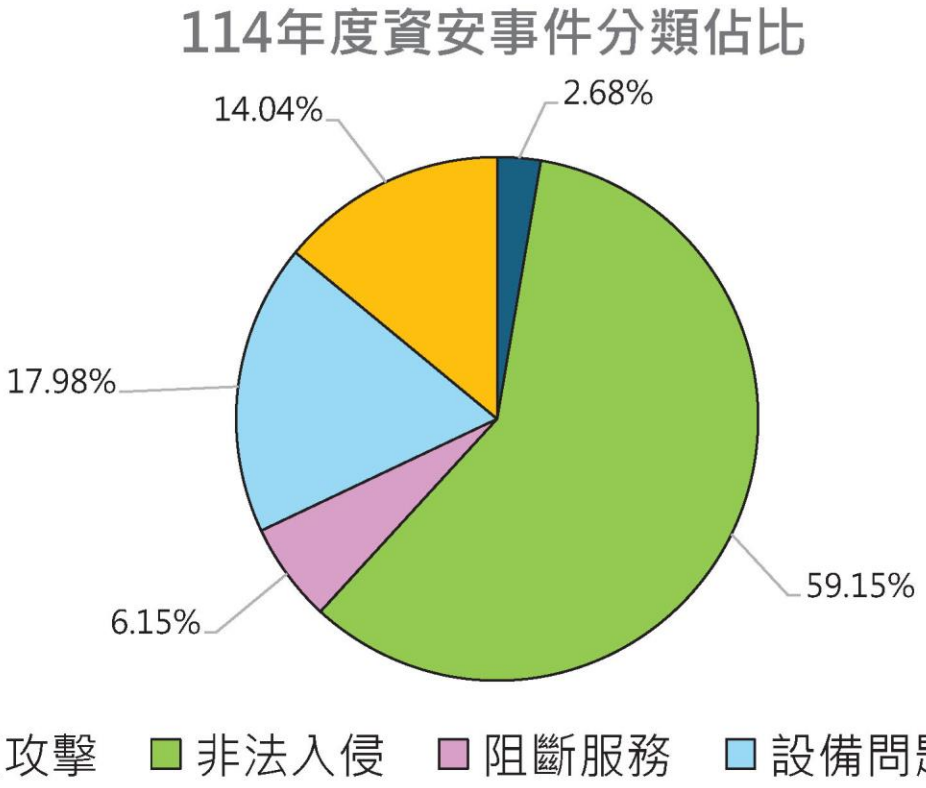

資料來源：資安趨勢部落格
https://blog.trendmicro.com.tw

# 數位發展部統計114年1月至9月資安事件

# 114年1月至9月資安事件(1/5)

## 納管機關資安事件通報統計

| 年度 | 事件數 | 1級事件 | 2級事件 | 3級事件 | 4級事件 |
|---|---|---|---|---|---|
| 114年(1-9月) | 634 | 529 | 80 | **25** | 0 |




**設備問題**

主因：多為設備異常/毀損、電力供應異常等

**非法入侵**

主因：為使用/下載來源不明之應用程式/套件，**主要為下載含有惡意程式之偽冒通訊軟體**

人為疏失

# 114年1月至9月資安事件(2/5)

## 3級以上資安事件樣態



**機密性**
**(共12件)**

- 雲端空間權限設定不當
- 人員疏失
- 社交工程
- 公文系統設定錯誤
- 網頁漏洞遭利用



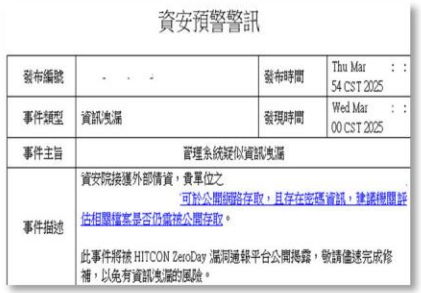
**可用性**
**(共13件)**

- 電力問題核心系統可用性中斷
- 系統遭入侵，影響核心業務(急診業務)
- 目錄權限設定錯誤，影響機關CI核心業務可用性
- 資料庫異常，無法於可容忍中斷時間內修復
- 網路設備異常，影響機關CI核心系統可用性

# 114年1月至9月資安事件(3/5)

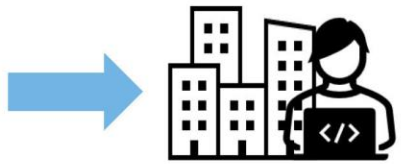
## 未即時處理資安預警警訊導致個資外洩

- 案係本署於114年3月發布**資安預警警訊(EWA)通知機關系統疑似存在弱點**，請機關儘速確認並進行必要應處，**惟機關遲至5月被通知後才進行處理，該系統已遭有心人士登入並瀏覽他人個資資料**，已造成個人資料外洩風險，爰通報3級資安事件。

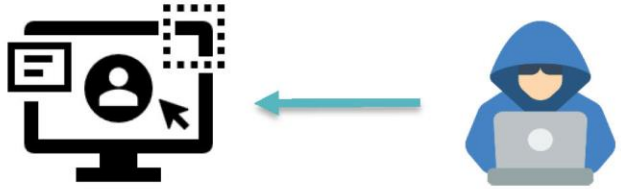


資安預警警訊

| 資安預警警訊 | | | |
|---|---|---|---|
| 發布編號 | - - - - | 發布時間 | Thu Mar : : 54 CST 2025 |
| 事件類型 | 資訊洩漏 | 發現時間 | Wed Mar : : 00 CST 2025 |
| 事件主旨 | 管理系統疑似資訊洩漏 | | |
| 事件描述 | 資安院接獲外部情資，貴單位之 可於公開網路存取，且存在密碼資訊，建議機關評估相關檔案是否仍需被公開存取。<br>此事件將被 HITCON ZeroDay 漏洞通報平台公開揭露，敬請儘速完成修補，以免有資訊洩漏的風險。 | | |



事發機關
未即時處理



導致系統已遭有心人士登入並瀏覽他人個資資料

### 建議防範措施

- 本署及資安院發布之EWA警訊，機關應儘速處理，**並依警訊內容進行檢視，若發現入侵事實(機密性、完整性或可用性受影響)，須依資安法進行通報**
- 資料保護，敏感資料加密儲存、**查詢過程遮蔽及最少揭露**

# 114年1月至9月資安事件(4/5)

## 雲端空間權限權限設定不當

- 機關辦理參訪活動報名時，透過QR CODE供民眾至雲端空間下載報名表，後續廠商將整理後含個資之報名資料與民眾可下載報名表存放於相同雲端空間內，**惟未設定雲端空間存取權限，導致民眾可掃描QR CODE後下載含個資之報名資料**，致敏感資訊外洩。

### 建議防範措施

- 機關辦理對外活動或公告所使用之報名方式時，**應確認其內容之妥適性及其資安管理措施**，避免因設定不當致資料外洩
- 使用雲端空間分享敏感資訊時，**檔案需加密，且資料夾應有合適權限管控**
- **注意廠商管理**，針對機敏資訊應加強管理與防護

# 114年1月至9月資安事件(5/5)

## 機關公務電話節費盒遭入侵及盜撥電話

- 案係某機關發現其公務電話遭不明人士盜打進行詐騙，經查該**公務電話係機關使用之網路電話**，比對撥話紀錄，發現有外部IP撥打情形，判斷應係設置於**機關內部之電話節費盒遭外部惡意登入**後，進行未授權撥號所致。




### 建議防範措施

- **使用高強度密碼**、並定期更新以及移除預設帳密
- **遵循「原則禁止，例外允許」原則**，進行存取限制管理
- 納入監控，**定期查看帳號登入及設備連線記錄**，避免異常情形
- **定期盤點更新狀態**，若設備已停產或不再提供安全性更新，應評估是否需進行汰換

# 警政署165全民防騙網—常見詐騙手法宣導

新聞快訊

# 刑事局掃蕩「一頁式廣告」查緝國內多家物流公司代付涉詐廣告費

發佈日期：2026-01-02 14:55
更新日期：2026-01-02 14:57

- 近年網購詐騙案件層出不窮，尤其以「超商包裹詐騙」手法最為猖獗，而「超商包裹詐騙」源頭多因民眾點擊「**一頁式詐騙廣告**」而下單遭詐，經刑事警察局追查「一頁式詐騙廣告」費用資金來源，為我國多家物流及倉儲公司所投放，遂與臺北市政府警察局成立專案小組，並報請臺灣桃園地方檢察署呂股王檢察官念珩指揮偵辦。
- 物流公司本業應為貨物運輸，卻頻繁且巨額地支付與本業不符之「廣告費用」，**本案經查我國共14家物流公司涉案，以「代收」貨款方式「代付」新臺幣達2.3億元之廣告費用，投放「一頁式詐騙廣告(減肥、玉鐲、茶葉及土蜂蜜)」，吸引民眾點擊廣告後加入假賣家line好友，下單後貨到付款進而發現為詐騙包裹**，全案涉及銀行法第29條地下匯兌罪嫌。
- 刑事警察局將持續執行一頁式詐騙廣告蒐報下架工作，並呼籲民眾勿隨意點擊一頁式詐騙廣告以免受騙；而對於勾結詐欺集團之不肖業者，亦會加強查緝，以保障民眾財產安全。

內政部警政署165全民防騙網
National Police Agency,Ministry of the Interior
165反詐騙諮詢專線

首頁 網站導覽

我要報案 我要檢舉 檢舉詐騙廣告

首頁 新聞快訊 涉詐資訊公告 檢舉詐欺報案 識詐宣導 常見詐騙手法 常見QA 檔案下載 相關連結



# 常見詐騙手法

2026-02-05 13:56
📌最新詐騙手法 請至165打詐儀錶板

2025-10-07 14:44
【新興手法】假贈送詐騙

2025-08-22 10:02
拘票註記「抗傳即拘」？假檢警詐騙的起手式

# 詐騙手法前 5 名

受理數 (件)　　財損 (元)

| | | 受理數(件) | 財損(元) |
|---|---|---|---|
| 1 | 網路購物詐騙 | 163 | 898.5 萬 |
| 2 | 假投資詐騙 | 39 | 1 億 35.2 萬 |
| 3 | 假交友(投資詐財)詐騙 | 32 | 5,855.5 萬 |
| 4 | 釣魚連結詐騙 | 17 | 111.9 萬 |
| 5 | 色情應召詐財詐騙 | 15 | 333.6 萬 |


雙證件被冒用？
當心假冒公務機關、假檢警詐騙
詐騙
不明來電指稱
涉及刑案(洗錢、毒品)
詐騙
要求加入檢警人員LINE
方便收取公文
10.25
Thursday
詐騙
要求雙證件
查證身分
詐騙
要求交付
帳戶、監管財產
提醒
地檢署不會通知帳戶監管、更不會到府收款！
接到可疑電話，請馬上掛斷並另撥打165！
更多防詐訊息 請搜尋
打詐儀錶板
https://165dashboard.tw/
內政部警政署 刑事警察局 CRIMINAL INVESTIGATION BUREAU
廣告

# 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

國立臺南大學
電子郵件社交工程演練資訊網

E-mail Social

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




ISMS PISMS

國立臺南大學資通安全宣導網 » 112年資通安全暨個人資料管理規範導入顧問輔導服務-宣導網

- 112年資通安全暨個人資料管理規範導入顧問輔導服務-線上教育訓練課程 >
- 教育體系資通安全管理規範驗證證書
- 中小學網路素養與認知網
- 資安漏洞警訊公告(國家資通安全研究院)
- 網路安全焦點新聞(中小學網路素養與認知網)

因應資通安全管理法要求，公務機關應於每年年底前完成資安法對資安教育訓練時數之要求。

1、資通安全專職人員：每人每年至少接受12小時以上之「資通安全專業課程訓練」或「資通安全職能訓練」。

2、資通安全專職人員以外之資訊人員：每人每2年至少接受3小時以上之「資通安全專業課程訓練」或「資通安全職能訓練」，且每年接受3小時以上之「資通安全通識教育訓練」。

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115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

單位處室中心名稱 *

您的回答

姓名 *

您的回答

# 感謝師長閱讀與配合
# 提升本校防範惡意電子郵件社交工程成效