教育部110上半年度電子郵件社交工程演練結果說明

教育部110上半年度電子郵件社交工程演練，本校受測人數為100名（含一、二級行政主管），未通過演練人員共34名，為了提高本校教職員工的資安意識，本中心將持續宣導資通安全的觀念外，**對於未能通過教育部演練人員，將列為日後加強資通安全宣導及教育訓練的對象**。將來這類性質的演練，教育部或行政院每年度會不定期地實施，因此，整理這次演練資料與結果，以及提供注意事項供本校使用者參考。

教育部演練目的及結果

教育部為強化教育機構教職員對資安意識的落實與對社交工程等攻擊行為的資安警覺意識，於2021年5月12日至2021年7月10日期間進行電子郵件社交工程演練，藉由模擬駭客寄送各種誘騙信件的手法，測試教職員點選各類誘騙信件的比率。
教育部合格標準：惡意郵件開啟率應低於10%以下；惡意連結（或檔案）點擊率應低於6%

測試信件摘要表

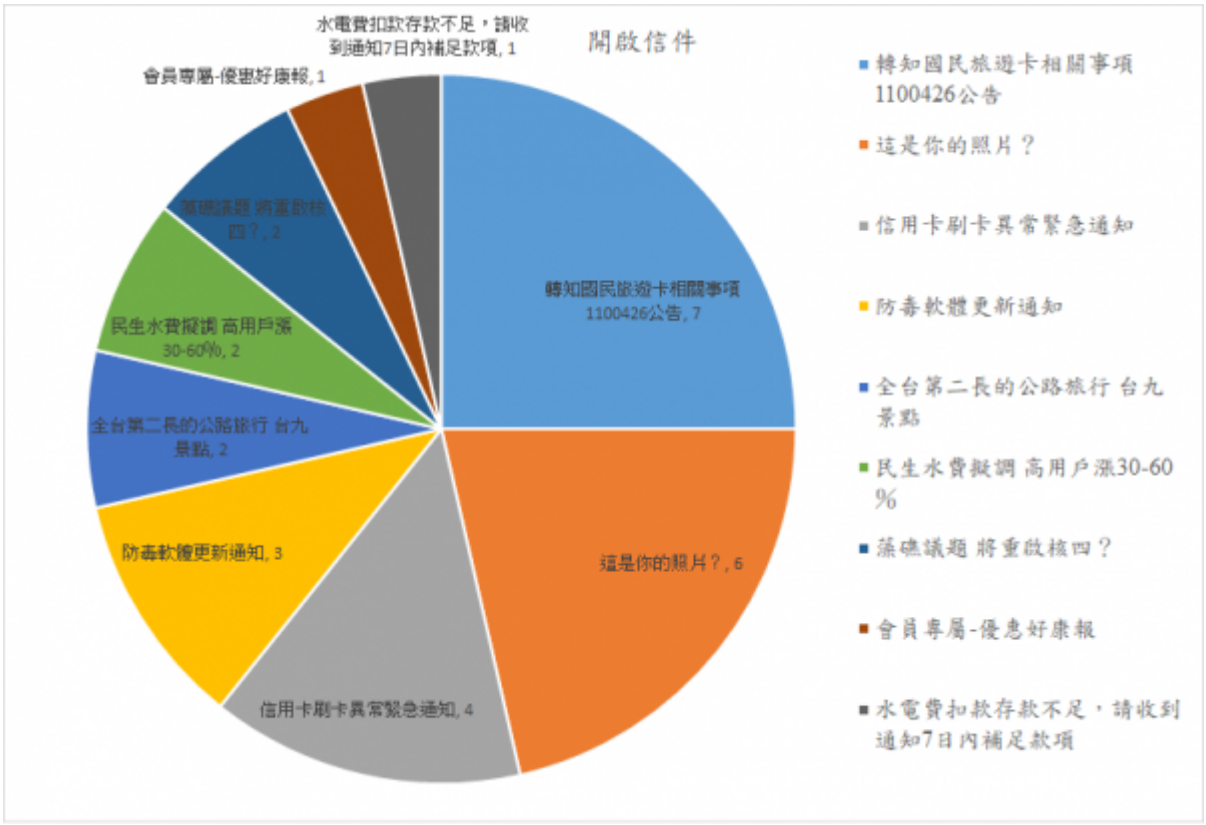
組別	信件類別	信件標題
Letter 1	生活消費	藻礁議題 將重啟核四？
Letter 2	生活消費	信用卡刷卡異常緊急通知
Letter 3	生活消費	水電費扣款存款不足，請收到通知7日內補足款項
Letter 4	公務相關	防毒軟體更新通知
Letter 5	生活消費	這是你的照片？
Letter 6	公務相關	轉之國民旅遊卡相關事項 1100426 公告
Letter 7	旅遊休閒	全台第二長的公路旅行台九景點
Letter 8	新聞時事	新冠變異種病毒株 恐憂帶來更大的疫情
Letter 9	生活消費	民生水費擬調 高用戶漲30-60%
Letter 10	生活消費	會員專屬-優惠好康報

測試定義

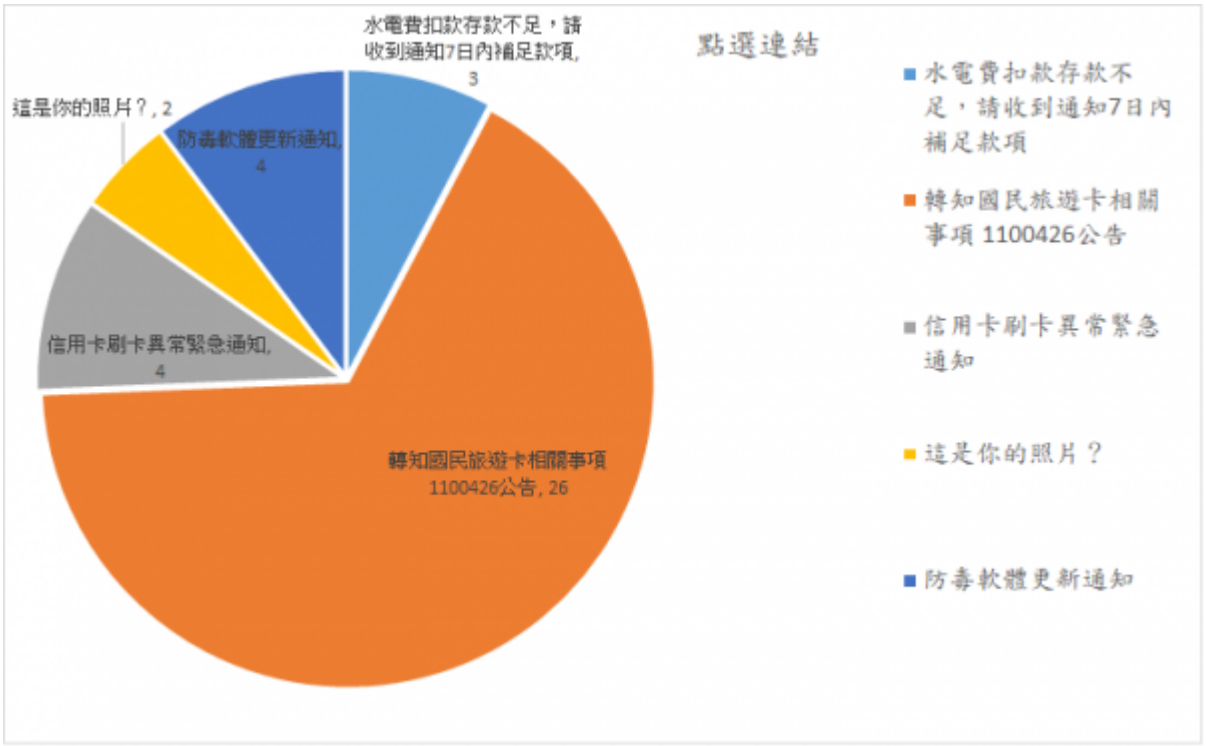
1. 信件開啟：偵測受測者於收到警覺性測試信件後，預覽或開啟信件圖片或內容，因而被記錄者。
2. 連結點選：偵測受測者於收到警覺性測試信件後，開啟信件並連結到信件中之URL或開啟附檔連結網址或附檔，因而被記錄者。

結果分析摘要

1. 開啟信件類別分析：以「轉知國民旅遊卡相關事項 1100426公告」最多。



2. 點擊信件連結作分析：以「轉知國民旅遊卡相關事項1100426公告」最多。



本校受測結果

教育部通知這次測試結果，本校共抽100人受測，開啟信件率14%。

一級單位 開啟信件

單位	人數	單位	人數
研究發展處	3	原子科學院	2
秘書處	2	工學院	1
主計室	1	全球事務處	1
竹師教育學院	1	電機資訊學院	1
學生事務處	1	環境保護暨安全衛生中心	1

教育部通知這次測試結果，本校共抽100人受測，點選連結率 34%。

一級單位 點選連結

單位	人數	單位	人數
學生事務處	5	總務處	5
研究發展處	4	秘書處	4
主計室	3	人事室	2
全球事務處	2	圖書館	2
人文社會學院	1	工學院	1
科技管理學院	1	原子科學院	1
教務處	1	清華學院	1
生命科學院	6	人文社會學院	4
電機資訊學院	1		

教育部通知這次測試結果，本校共抽100人受測， 3%。

一級單位 開啟附檔

單位	人數	單位	人數
總務處	1	綜合業務組	1
校園規劃室	1		

使用者注意事項

電子郵件社交工程型攻擊的目的在於誘騙收信者提供個人資料(如：帳號、密碼)，或**引誘收信者透過下載方式來執行以圖片、連結、夾檔所偽裝的惡意軟體(malware)**，讓電腦中毒成為入侵者所控制的殭屍網路電腦(botnet)。

由於這類的攻擊，如：下載圖片、點選連結，實際惡意軟體的資料是由使用者電腦直接向提供者下載取得，並不會經過郵件伺服器的防毒機制，即使過濾夾檔也有零日病毒(Wzero-day virus)的問題，在郵件伺服器端僅能過濾已知的病毒，因此，**最佳防範這類社交工程型態攻擊的方法，就是使用者要有資安警覺**，收到電子郵件時，注意下列幾件事：

1. **不要開啟不明信件**：開啟信件前，務必先檢視寄件者資料，如有疑問，千萬不要開啟。最好**設定郵件軟體安全性為「不要自動下載圖片」**，以免不小心按到開啟信件時，會自動下載到有問題的檔案，而讓電腦產生安全漏洞。
2. **不點擊不明信件內的連結**。
3. **不開啟不明信件的夾檔**。

其他參考資料

* 郵件軟體安全性設定

- 各種郵件軟體不下載遠端圖片的設定方式