社交工程演練專區

近年來，教育機構屢遭網路駭客鎖定，以各種偽造的電子郵件騙取教職員的帳號密碼或植入勒索軟體，對校務運作與個人資料安全造成嚴重威脅。

為了強化本校整體的資安防禦體系，並落實《資通安全管理法》等相關規定，資訊中心將於 115 年 4 月 20 至 4 月 26 日實施全校性的「電子郵件社交工程演練」。

一、 演練的意義與用途

數位防護的「消防演習」： 就如同我們定期舉辦的實體消防演練一樣，本次演練旨在測試當真正的網路攻擊發生時，我們的防禦與應變能力。

提升資安意識： 透過模擬真實的攻擊情境，協助同仁在日常繁忙的公務中，培養辨識釣魚信件的敏銳度。

檢視防護現況，作為教育訓練依據： 演練的統計結果將僅用於整體資安風險評估，並作為未來規劃資安宣導的參考。

二、 演練實施方式

資訊中心在演練期間內，將不定時發送「模擬的釣魚電子郵件」至同仁的公務信箱。

這些信件的主旨可能會偽裝成：系統維護通知、薪資單查詢、假期的重要公告、甚至是熱門時事新聞。

信件內容會包含模擬的「惡意連結」或「附加檔案」。（註：演練用的連結與檔案皆經過安全處理，絕對無害，不會感染您的電腦或竊取真實密碼。）

三、同仁注意事項

落實「停、看、查」原則： 收到要求您點擊連結、輸入帳號密碼或下載附件的信件時，請務必先確認「寄件者」是否正確，並對帶有「急迫性」或「威脅性」語氣的信件保持高度警戒。

不慎點擊請勿驚慌： 若您在演練期間不慎點擊了測試信件的連結，系統可能會

跳轉至「資安宣導教育頁面」。這表示您已參與了本次機會教育，請詳細閱讀該頁面的防護建議即可，您的設備安全無虞。

四、懇請配合事項

請勿公開「暴雷」： 為了維持演練的真實性與準確度，請讓每位同仁都有機會親自進行判斷與練習。

🚨 主動通報機制： 若您在日常工作中（不論是否為演練期間），發現任何疑似詐騙或釣魚的信件，請勿點擊任何內容，並請直接填寫線上通報表單，資訊中心將會盡速處理：

👉 【資安事件線上通報表單】：https://forms.gle/ssLc2RECVu72Ch1y5