114 年度社交工程演練 — 課後測驗「答案解說」

本文件提供 10 題測驗之正確答案與簡要說明，可作為教育訓練講義或 ISO 27001 稽核佐證資料。

一、是非題（7 題）

1. 社交工程是指駭客透過技術手段入侵電腦系統的攻擊方式。

答案：錯誤
解說：社交工程重點在「人」的弱點與心理操弄，例如誘騙、偽裝、權威施壓，並非以技術漏洞為核心。

2. 郵件標題包含「獎金」或「公告」就能確定是公司信件。

答案：錯誤
解說：標題容易被仿造。需核對寄件人網域、回覆位址、超連結實際 URL、附件來源與內容一致性。

3. 釣魚郵件常利用假冒主管、銀行名義誘使員工點擊連結。

答案：正確
解說：常見社交工程情境包括假冒主管急件、金融機構驗證、知名服務重設密碼等，利用權威與急迫感提升點擊率。

4. 若收到疑似釣魚的郵件，可立即轉寄給同事幫忙確認是否安全。

答案：錯誤
解說：轉寄可能擴散惡意連結或附件。應使用公司規定的通報機制回報資安/IT 單位並保留證據。

5. 公司進行社交工程演練的目的，是為了檢測員工的資安警覺與通報流程是否正確。

答案：正確
解說：演練可驗證識別能力、通報效率與流程可行性，作為改善教育訓練與制度的依據。

6. 在社交工程防護中，「驗證寄件者真實身分」是最有效的第一步。

答案：正確
解說：先確認人再處理事。可透過第二通道（如電話/Teams）核實、檢查寄件網域與 SPF/DKIM/DMARC 標記、比對以往通信紀錄。

7. 若誤點釣魚連結，只要電腦沒有異常就不需通報。

答案：錯誤
解說：帳密可能已在連結頁被蒐集，或植入延遲發作的惡意碼。需立刻通報、變更密碼並依流程檢查主機。

二、選擇題（3 題）

8. 下列何者屬於社交工程常見手法？

正確答案：B（假冒主管要求提供資料）
解說：A/D 偏技術攻擊，C 與資安攻擊無關；B 為典型情境式誘騙。

9. 當懷疑信件為釣魚郵件時，應採取下列何種行為？

正確答案：C（通報 IT 單位）
解說：應依內規通報與暫停互動。A 會提高風險，B 可能暴露更多資訊，D 直接刪除會喪失取證線索。

10. 社交工程演練結果的主要用意為：

正確答案：C（強化員工資安意識）
解說：演練目的在教育與改善流程與行為，而非測試郵件伺服器或增加郵件量。