《資通安全概論》

一、請說明何謂社交工程攻擊（Social Engineering Attack）？並詳述常見的社交工程攻擊方式及相對應的防護措施。（25分）

試題評析	社交工程已經是很常見的攻擊模式，像詐騙案件雖然一直發生，但是手法卻是日新月異，從以前的裝熟、猜猜我是誰，到現在的AI深偽辨識，因此能回答到目前社交工程攻擊趨勢與有效防止手法，是得高分的關鍵。
考點命中	《高點•高上資通安全講義》第一回，金乃傑編撰，第三章第三節，頁96～97。

答：

1.社交工程是利用人性弱點，應用人性對於新事物、熱門八卦話題與群體關係互動，讓人們對於敏感性資料保護放下戒心，攻擊者利用人性互動達到目的技術。目的通常為金錢、商業機密或是政府敏感性資料，由於是透過取得合法認證者的信任，殺傷力有時可能比駭客直接突破資通安全防護，遂行非法存取的效率來得好。

2.常見攻擊方式：

(1)假冒身分：假冒為親人、朋友，需要點選認證碼或是匯款。

(2)假冒合法網站：假冒為銀行公司，可以結合DNS攻擊，讓使用者輸入網路銀行密碼。

(3)假冒公務人員：假冒假檢警，由於是公部門具有可信力且針對一般人不想扯入司法案件特性，至今仍時常耳聞。

(4)廣發訊息：廣發電子郵件、簡訊，透過優惠廣告、費用未繳、購物失敗等訊息，讓使用者點擊，進而獲取資訊。

3.近年來趨勢：

(1)虛擬貨幣：假冒幣商、假的錢包APP，當輸入「特徵碼」或是錢包私鑰早已被攻擊者竊知，進而達到移轉財產目的，由於加密貨幣的隱密性，使得追蹤犯罪更加困難。

(2)深偽技術：運用AI進行變臉、變聲音，使得陌生人可以變成親近好友，縱使視訊也難以看出破綻，進而獲取個人相關敏感資料。

(3)交友軟體：透過交友網站或是交友APP，認識浪漫的異國戀，暢談美好未來，結果只是攻擊者的話術。

防範手法：

(1)提高警惕：對於來路不明的訊息、陌生的電話、電子郵件多加留意，尤其對方試圖想讓受害者匯款、取得資訊或是操作相關系統。

(2)使用雙因子認證：啟用指紋、手機簡訊碼驗證，並強化密碼強度管理。

(3)更新作業系統、軟體與憑證，減少可能已知的漏洞攻擊。

(4)確認網站網址，避免進入釣魚網站的假頁面；此外，盡可能選用有https或TLS的網站，確保通訊資料未被洩漏。

(5)組織對於可上網的網站採用白名單限制，確保可上網網站為合法且安全。

(6)政府組織與電信業者對於手機與郵件廣發簡訊、廣告與電子郵件的發送者，必須實名制或是具有自然人憑證，以避免有心人士進行釣魚。

(7)對於AI深偽辨識，則可以透過家裡擺設、曾經發生過的事、或是生活發生點滴，採用是與否交叉驗證，確認談話者是否可以判斷哪些事有無發生過。

二、請說明基於密碼學演算法的數位簽章（Digital Signature）具有那些學理特性？並詳述實務應用領域需要使用可信賴的憑證機構（Certification Authority,CA）依法簽發的憑證（Certificate）來製作數位簽章之原因？（25分）

試題評析	此題考的是數位簽章，是傳統的資安考題，實務應用於如公文系統傳簽已成熟，然而實務應用如何得到高分要與時勢能結合。數位部與經濟部不久前推動電子簽章修法，除了認定法律效力定位，主要是要解決網路廣告的審核成本，實名制審核成本高且程序冗長，如同銀行的KYC，未來網路廣告有詐騙行為如同實體簽名，可以找到源頭並下架，解決日益增加的詐騙問題。

考點命中	1.《高點•高上資通安全講義》第一回，金乃傑編撰，第二章第一節，頁5～6。 2.《高點•高上資通安全講義》第一回，金乃傑編撰，第二章第七節，頁58～60。

答：

數位簽章：為數位憑證的持有者，對於文件簽名之後所產生的數位訊息，由於這個數位訊息是由憑證持有者用私鑰簽署的，因此可以判斷何人所簽，與原始訊息為何。

數位簽章=原始訊息+ E私鑰(雜湊函數(原始訊息))，接收到的人可以用憑證的公鑰進行驗證

特性：

(1)完整性：確保原始訊息未被修改。

(2)身分鑑別：確認傳送者身分。

(3)不可否認：因為是用私鑰傳送，除了憑證持有人外，沒有人擁有私鑰，因此無法否認曾傳送過訊息。

可信賴的憑證機構：以政府公開金鑰基礎建設GPKI為例，CA的角色是為憑證之正確性作擔保，憑證內容有公鑰、私鑰與個人信息，乃為具有公信力第三者，可以達到資訊安全中的機密性、完整性、身分鑑別性、不可否認性的要點，未來若交易之間有糾紛，可以釐清責任歸屬。

實務應用：由於目前5G網路日益完善，雲端、大數據技術已經成熟，資訊爆炸的今日，提供了機器學習與人工智慧發展的舞台，然而隨之而來的弊端為廣告詐騙、人頭帳戶詐騙案件的暴增。

目前透過人工審核機制過濾可疑的廣告詐騙與帳戶，然而人工審查冗長、成本高且與網路開放性相違背，因此若能在投放廣告後，先驗證數位簽章，可以知道這個廣告或是投資人為何者，內容是否有竄改，傳送過程中使用CA所發行的公開金鑰進行加密，確保機敏資訊，如信用卡號等不會外洩，若為惡意詐騙廣告與人頭戶，司法機關也可以回頭追溯投放廣告時數位簽章的身分，確保網路環境的效率、低成本與資訊安全。

三、若網站系統設計不當，將可能遭受SQL注入攻擊（SQL Injection）。請說明產生SQL注入攻擊的可能原因，並詳述防禦SQL注入攻擊的系統改善方案。（25分）

試題評析	SQL Injection 已經是傳統考古題，2023公布的OWASP十大弱點中，和XSS攻擊合併為第三，因此國家考試上仍會出現。對於一般有讀到的考生並不會太困難，高分關鍵仍是要舉出SQL injection可能的後果，防範可行手法至少一種程式語言或是通用的方法。
考點命中	《高點•高上資通安全講義》第一回，金乃傑編撰，第三章第四節，頁108。

答：

SQL injection透過不預期的SQL語句，進而達到存取非自身權限所擁有的資料，或是進行惡意的操作如刪除資料庫或是修改，達到攻擊的目的。

範例：

SELECT * from students where id='sun' AND password='' or 1='1' --;

SQL injection 防範：

1.以Java為例，使用參數化查詢，

```
PreparedStatement stat = conn.prepareStatement("Select * From A  Where id = ? AND password = ?");
stat.setString(1, "sun");
stat.setString(2, "get");
stat.executeQuery();
```

setString()第一個值是位置，第二個參數是要置換的值。

2.以php為例，可以使用htmlentities()或是mysqli real_escape_string()進行過濾特殊符號。

3.使用stored procedure取代程式碼中組合式的SQL，

範例：exec預存程序A　@變數a ='內容a',@變數b ='內容b'

4.避免將原始資料庫錯誤訊息提供給使用者。

5.送到資料庫前，使用正規表示式，對輸入資料進行有特殊字元驗證。

6.最小權限原則，假如使用者A只需要「查詢」某個資料表，則不需要開放整個資料庫權限，也

可以使用資料庫view功能；若只需要select，就不應該給予alter、delete、drop等功能。

四、請詳述至少兩種常用於防止洩露個人隱私或機敏資料的去識別化（Deidentification）方法。（25分）

試題評析	隨著人工智慧的應用，機器學習或是生成式網路仰賴資料的輸入，因此政府機關的開放式資料、網路的內容爬蟲未來會越來越多；因此如何將資料合法應用又不洩漏個人隱私，為未來提供人工智慧發展的重要議題。
考點命中	《高點・高上資訊管理與資通安全講義》第一回，蕭老師編撰，頁17～18。

答：

去識別化：

1.K-匿名(k-anonymity)：

(1)單元抑制：將部分資料屬性進行不顯示或是以”*”號代替。

(2)一般化：是對資料屬性進行範圍更廣、特定數值改區間、或抽象的描述，且不失原意，與原有屬性表達必須具有實質相同意義。例如：將年齡23歲，以21~30 歲區間顯示。

2.差分隱私(differential privacy)：是一種保護個人資料隱私的手段，主要方式是透過加入「雜訊」與移除可辨別資料(例如：只有一個人的薪水為10萬)，加入雜訊與移除後的資料統計值與原始資料機率分布上差異很小。

提供「查詢」資料庫的統計特徵而不公開個人資訊與原始資料，可以實現共享資料、機器學習、資料探勘等領域，最高的隱私標準，Google、Apple 公開資料時使用此方法。

例如：公司獎金聽說最高的是「薪水是獎金一半」，

Jack薪水10萬，獎金20萬，

增加幾筆相近的「雜訊」資料，並將Jack移除，不提供查詢。