《資訊管理與資通安全概要》

一、請回答下列資訊安全問題：（每小題15分，共30分）

(一)請說明變臉詐騙（Business Email Compromise），並提出預防方式。

(二)請說明勒索病毒，並提出預防方式。

試題評析	第一題看似沒遇過，老師建議同學可以從英文下手並嘗試理解其意義就可解決此題，運用到的概念和老師上課補充不謀而合。本題第二題屬於攻擊的基本概念，只要對於攻擊方式有基本認知，便可以輕鬆應付勒索軟體的基本定義與防範，對同學不構成威脅。
考點命中	《高點‧高上資訊管理與資通安全講義》第三回，蕭老師編撰，頁58-59。

答：

(一)變臉詐騙往往從攻擊者入侵企業高階主管郵件帳號或任何公開郵件帳號開始。通常經由鍵盤側錄惡意軟體或網路釣魚（Phishing）手法達成，攻擊者會建立類似目標公司的網域或偽造的電子郵件來誘騙目標提供帳號資料。在監控受駭電子郵件帳號時，詐騙者會試著找出進行轉帳及要求轉帳的對象。詐騙者通常會進行相當的研究，尋找財務高階主管變動的公司，高階主管正在旅行的公司或是進行投資人電話會議來製造機會以進行騙局。其常見的方法有以下三種

1.透過偽造的郵件、電話或傳真要求匯款給另一個詐騙用帳戶：這個手法也被稱為「偽造發票騙局」、「供應商詐騙」和「發票變造騙局」，通常跟有供應商關係的企業有關。詐騙者透過偽造的郵件、電話或傳真要求匯款給另一個詐騙用帳戶。

2.詐騙者自稱為高階主管（CFO、CEO、CTO等）、律師或其他類型的法定代表：在這個手法中，詐騙者自稱為高階主管（CFO、CEO、CTO等）、律師或其他類型的法定代表，聲稱要處理機密或有時效性的事情，要求匯款至他們所控制的帳戶。在某些案例中，欺詐性的匯款轉帳要求直接到金融機構，指示要緊急發送資金到一家銀行。這種騙局也被稱為「CEO詐騙」、「企業高階主管詐騙」、「偽造身分」和「金融企業匯款詐騙」。

3.駭客入侵員工的電子郵件帳號：跟其他兩個手法類似，駭客入侵員工的電子郵件帳號，接著用此帳戶要求發票付款給詐騙者所控制的銀行帳戶。郵件送至員工聯絡人列表上所找到的多個供應商。在廠商追查發票付款狀態前，企業可能不會察覺詐騙發生。

常見且較為有利的防範方式為：

1.仔細檢查所有的電子郵件：小心來自高階主管送來的不尋常郵件，因為它們是用來誘騙員工去緊急動作。檢視要求資金轉移的電子郵件以確認該請求是否正常。

2.教育和訓練員工：雖然員工是公司最大的資產，當提到資訊安全，他們往往也是最脆弱的一環。依照公司的最佳實作來培訓員工。提醒他們遵守公司政策是一回事，但養成良好的安全習慣是另一回事。

3.供應商付款位置改變要由公司人員進行第二層簽核來加以確認：了解客戶的習性，包括細節和付款背後的原因。

4.使用手機驗證來確認資金轉移請求以作為雙因子認證：使用已知的熟悉號碼而非來自電子郵件中所提供的內容。

(二)勒索病毒是一種特殊的惡意軟體，被歸類於「阻斷存取式攻擊」（denial-of-access attack）。其攻擊方式大概可以分為「僅是單純地將受害者的電腦鎖起來」與「系統性地加密受害者硬碟上的檔案」，這個攻擊方式不會立即讓使用者感受到，惡意軟體會在背地裡悄然運作，直到系統或資料鎖定機制佈署完成。部署完成後，才會告訴使用者資料遭上鎖並藉此勒索贖金以取回對電腦的控制權，或是取回受害者根本無從自行取得的解密金鑰以便解密檔案。

其通常透過木馬病毒的形式傳播，例如透過假冒成普通的電子郵件等社會工程學方法欺騙受害者點擊連結下載，主要會將自身掩蓋為看似無害的檔案。或是透過路過式攻擊，也就是使用者瀏覽網頁或惡意廣告就會中毒。預防方式可為：

1.有感染跡象時立即斷網、關機並暫時停止該帳號的網路存取登入權限

2.使用防毒軟體

3.定期備份重要檔案

4.定期更新軟體
5.避免點選不明連結
6.組織提供不間斷的員工警覺性訓練
7.控管共用資料夾的存取權限，例如：不提供寫入權限

二、請回答下列資訊安全弱點相關問題：（每小題10分，共20分）
(一)請說明OWASP TOP 10 用途。
(二)請說明Injection 弱點與影響。

試題評析	此題為資訊安全的基本題型，同學只要依照講義上的說明，依照Injection的特性並回答即可。
考點命中	《高點・高上資訊管理與資通安全講義》第三回，蕭老師編撰，頁105-106。

答：
(一)開放網路軟體安全計畫，簡稱 OWASP（Open Web Application Security Project），OWASP是一個開放社群、非營利性組織，其主要目標是研議協助解決網路軟體安全之標準、工具與技術文件，長期致力於協助政府或企業瞭解並改善應用程式的安全性。從數以百計的組織和超過10萬個實際應用程式和API中收集的漏洞，並根據這些流行數據選擇和優先排序出前10大威脅與漏洞，且結合了對可利用性、可檢測性和影響程度的一致性評估而形成。OWASP Top10主要目的，是將最常見的網路應用系統安全弱點，教育開發者（Developers）、設計者（Designers）、架構師（Architects）和組織（Organizations），提供基本的方法保護防止這些弱點，是軟體開發安全計劃最好的開始。
(二)注入攻擊（Injection）
是發生於應用程式與資料庫層的安全漏洞，攻擊者在網頁可以輸入資料的地方嘗試填入不合法的語法，其目的為猜測網頁設計者背後撰寫語法的邏輯，利用該欄位搭配自己的語法組合成一個可以造成對網頁有害的攻擊指令，像是推測欄位數，table的名字，SQL的版本資訊，試著去拼湊輸入一條SQL指令，輕則刪掉資料庫，重則竊取全部的個資。而針對注入攻擊，系統在開發時需要注意：
(1)不要將錯誤訊息給管理者以外的人看到，以避免攻擊者獲得更多的攻擊資訊。
(2)對於使用者個帳號權限需要有控管機制。
(3)需要對使用者所有輸入的字串進行合法性檢查。

三、根據行政院國家資通安全會報技術服務中心之資通系統委外開發RFP資安需求範本，請列舉並說明兩項系統與服務獲得時所需的安全需求。（30分）

試題評析	此題主要考資訊系統委外開發之需求，同學若是沒有看過行政院國家資通安全會報裡面的詳細內容，也不用特別緊張，只需要依照課程講義來答題即可。
考點命中	《高點・高上資訊管理與資通安全講義》第二回，蕭老師編撰，頁12-14。

答：
(一)建立帳號管理機制，包含帳號之申請、開通、停用及刪除之程序：資通系統之帳號應透過正式的帳號申請程序所建立，完成開通審核程序始能使用，因此系統應具備帳號管理機制，可對系統帳號進行申請、開通、停用或刪除之行為。
(二)對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化，使用者之權限檢查作業應於伺服器端完成：機關應明確訂定資通系統之存取限制、組態需求、連線需求，並將這些資訊文件化，以供日後查檢。應於伺服器端實作權限檢查機制，並預設禁止任何未通過權限檢查之存取行為，以避免被使用者繞過。
(三)資通系統產生之稽核紀錄應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，並採用單一日誌紀錄機制，確保輸出格式之一致性：稽核紀錄應詳細描述所觸發的事件，包含人、事、時、地、物等關鍵資訊，宜包含：使用者帳號(避免個資類型)、時間、執行之功能或存取之資源名稱、事件類型或優先等級、執行結果或事件描述、事件發生當下相關物件資訊、網路來源與目的位址，以及錯誤代碼等。盡可能採用單一的 Log 機制，如同一伺服器軟體應產出相同格式之稽核紀錄等，以便於

事件比對與追查。

四、請說明資料庫交易要符合那四個特性，並敘述其意涵。（20分）

試題評析	此題考純粹的資料庫ACID概念，將基本概念列出即可，也可以依照資料庫的基本需求依序描述出來就可解答。

答：

(一)Atomicity（原子性）- 在資料庫的每一筆交易中只有兩種可能發生，第一種是全部完全(commit)，第二種是全部不完成(rollback)，不會因為某個環節出錯，而終止在那個環節，在出錯之後會恢復至交易之前的狀態，如同還沒執行此筆交易。

(二)Consistency（一致性）- 在交易中會產生資料或者驗證狀態，然而當錯誤發生，所有已更改的資料或狀態將會恢復至交易之前。

(三)Isolation（隔離性）- 資料庫允許多筆交易同時進行，交易進行時未完成的交易資料並不會被其他交易使用，直到此筆交易完成。

(四)Durability (持續性）- 交易完成後對資料的修改是永久性的，資料不會因為系統重啟或錯誤而改變。