110 年公務人員普通考試試題

類　科：資訊處理
科　目：資訊管理與資通安全概要

甲、申論題部分：

一、請回答列資訊安全問題：（每小題 15 分，共 30 分）

㈠請說明變臉詐騙（Business Email Compromise），並提出預防方式。

㈡請說明勒索病毒，並提出預防方式。

【解題關鍵】
《考題難易》：★★
《破題關鍵》：資訊安全態樣題，參考資通安全講義資安技術類似題（105 調查局特考類似題、即可作答。
《命中特區》：舊版資管與資通安全講義 P650（命中（二））、P652（魚叉式釣魚攻擊為㈠之方式之一）

【擬答】

㈠變臉詐騙（Business Email Compromise，又稱商務電子郵件入侵），是一種網絡犯罪形式，它使用電子郵件欺詐來攻擊企業、政府和非營利組織，以達到特定結果，從而對目標組織產生負面影響。通常攻擊會通過發送欺騙性電子郵件（或一系列欺騙性電子郵件）來欺騙組織內的特定員工角色，這些電子郵件以欺詐方式代表高級同事（CEO 或類似人員）或受信任的客戶。 電子郵件將發出指令，例如批准付款或發布客戶數據。這些電子郵件通常使用社交工程來誘騙受害者向欺詐者的銀行賬戶匯款。其預防方式如下：

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。了解你客戶的習性，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。
5. 如果你懷疑自己成為 BEC 郵件的目標，立即向執法部門回報。

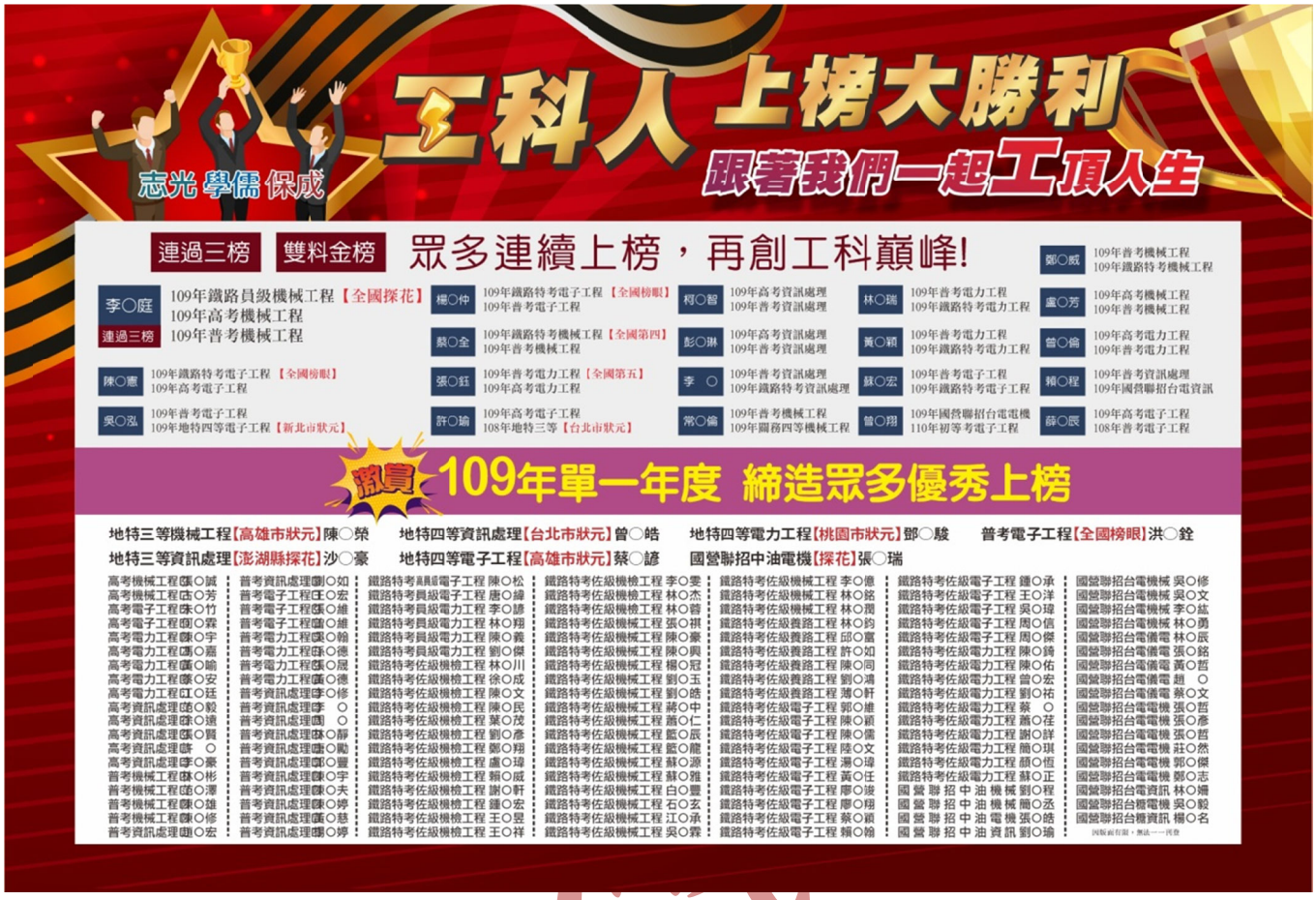
㈡勒索病毒是一種特殊的惡意軟體，屬於阻斷存取式攻擊，但攻擊手法與其他病毒不同。勒索病毒可以將受害者的電腦鎖起來，或是系統性的加密受害者硬碟上的檔案後。要求受害者繳納贖金以取回對電腦的控制權，或是取回受害者根本無從自行取得的加密金鑰。勒索病毒通常透過木馬病毒的形式傳播，將自身為掩蓋為看似無害的檔案。也可以透過路過式下載（隱藏式下載、偷渡式下載、強迫下載，網頁掛馬）攻擊，瀏覽惡意網頁或惡意廣告就會中毒。其預防方式：

1. 發生感染徵狀立即斷網、斷電（馬上關機），關閉帳號，暫時停止該帳號的網路存取登入權限。
2. 要定期備份重要的檔案。
3. 要定期更新修補作業系統與應用程式的漏洞。
4. 不開放共享資料夾寫入權限。

5. 不共用帳號。

6. 只打開信任的郵件，不隨意打開未知來源信件的連結以及附件。

7. 使用安全評價較高的瀏覽器。



二、請回答下列資訊安全弱點相關問題：（每小題 10 分，共 20 分）

㈠請說明 OWASP TOP 10 用途。

㈡請說明 Injection 弱點與影響。

【解題關鍵】

《考題難易》：★★

《破題關鍵》：資訊安全弱點基本題，只要參考補充講義 OWASP 與其中 Top1 弱點（injection 攻擊）即可作答。

《命中特區》：資通安全講義中 OWASP Top10。

【擬答】

㈠開放式 Web 應用程式安全專案（OWASP）是一個線上社群，在 Web 應用安全領域提供免費的文章，方法，文件，工具和技術。OWASP TOP 1 旨在通過辨識組織面臨的一些最重要的風險來提高對應用程式安全性的認識。蒐集各種網頁安全漏洞，歸納出好發且容易攻擊的弱點，彙整為十大資安問題、排名、防範措施。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。

㈡injection 弱點，是發生於應用程式之資料庫層的安全漏洞，因為使用者提供的資料傳輸到一個 interpreter，此被當成指令（Command）或是查詢（Query）。攻擊者就能用惡意的資料欺騙 interpreter，而達到執行指令或是竄改資料的目的。在輸入的字串之中夾帶 SQL 指令，在設計不良的程式當中忽略了檢查，那麼這些夾帶進去的指令就會被資料庫伺服器誤認為是正常的 SQL 指令而執行，因此遭到破壞或是入侵。

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）

【解題關鍵】
《考題難易》：★★★
《破題關鍵》：資通安全管理法相關考題，參考資通安全責任等級分級辦法附表十資通系統防護基準中系統與服務獲得項下作答。

【擬答】

㈠發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息

系統應設計錯誤處理機制，當系統發生錯誤時，儘可能採取錯誤代碼或簡短訊息呈現，避免將詳細或除錯用訊息直接顯示於使用者頁面，以防被攻擊者用來刺探系統內部資訊，或根據錯誤訊息推測出系統可能之弱點。確保系統所有功能的程式碼，在程式的進入點之後，盡可能採用程式語言的 try-catch 陳述，捕捉可能發生的錯誤與例外狀況。另外，採用程式語言的 finally 陳述，確保將該段功能程式碼所使用的資源正確釋放。

㈡具備系統嚴重錯誤之通知機制

系統應區分錯誤等級，若發生嚴重等級錯誤時，採用電子郵件或簡訊等通知機制，使系統管理員或相關人員可及時掌握狀況，以利進行後續處理。

㈢資通系統相關軟體，不使用預設密碼

系統相關軟體元件或組態設定若有使用預設密碼，應於系統正式上線前變更完畢。

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）

【解題關鍵】
《考題難易》：★
《破題關鍵》：資訊技術基本題，參考講義第 3 章 101 地方四等類似題即可輕鬆作答。
《命中特區》：資管講義 P224 完全命中。

【擬答】

㈠單一性（atomicity）：交易是執行的單一單位，不是全部做完就是全部不做。

㈡一致性（consistency）：一個正確執行的交易會讓資料庫從一個一致的狀態轉換到另一個一致的狀態，也就是說此種轉換會保留一致性。雖然在中間點時可能不一定保留一致性，但並不會影響其結果。

㈢孤立性（isolation）：交易間會相互孤立，也就是說直到交易到達確認（commit）狀態，都不會讓其對資料庫的改變影響其他的交易，也就是說此種改變對其他交易是不可見的（invisible）。

㈣耐久性（durability）：當交易到達確認（commit）狀態，其對資料庫的改變就不會因為後續資料庫的失敗而喪失。