

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）

(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。

【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(一)之方式之一）

【擬答】

(一)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。

(二)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。



工科人 上榜大勝利

跟著我們一起工頂人生

連過三榜 雙料金榜 眾多連續上榜，再創工科巔峰!

<p>李○庭 109年鐵路員級機械工程【全國探花】 109年普考機械工程 連過三榜</p> <p>陳○應 109年鐵路特考電子工程【全國榜眼】 109年普考電子工程</p> <p>吳○泓 109年普考電子工程 109年地特四等電子工程【新北市狀元】</p>	<p>楊○仲 109年鐵路特考電子工程【全國榜眼】 109年普考電子工程</p> <p>蔡○全 109年鐵路特考機械工程【全國第四】 109年普考機械工程</p> <p>張○廷 109年普考電力工程 109年普考電子工程</p> <p>許○諭 109年普考電子工程 108年地特三等【台北市狀元】</p>	<p>柯○豐 109年普考資訊處理 109年普考資訊處理</p> <p>彭○琳 109年普考資訊處理 109年普考資訊處理</p> <p>李○ 109年普考資訊處理 109年鐵路特考資訊處理</p> <p>常○倫 109年普考機械工程 109年普考機械工程</p>	<p>林○璵 109年普考電力工程 109年鐵路特考電力工程</p> <p>黃○穎 109年普考電力工程 109年鐵路特考電力工程</p> <p>蘇○宏 109年普考資訊處理 109年鐵路特考資訊處理</p> <p>曾○翔 109年普考電子工程 110年初等考電子工程</p> <p>薛○辰 109年普考電子工程 108年普考電子工程</p>
---	--	--	--

109年單一年度 締造眾多優秀上榜

<p>地特三等機械工程【高雄市狀元】陳○榮</p> <p>地特三等資訊處理【澎湖縣探花】沙○豪</p>	<p>地特四等資訊處理【台北市狀元】曾○皓</p> <p>地特四等電子工程【高雄市狀元】蔡○諱</p>	<p>地特四等電力工程【桃園市狀元】鄧○駿</p> <p>國營聯招中油電機【探花】張○瑞</p>	<p>普考電子工程【全國榜眼】洪○銓</p>
---	---	--	-------------------------------

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。

【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】

(一)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。

(二)injection 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】

- (一)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。
- (二)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。
- (三)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。



公職工科+國營事業

1+1 更有力

準備公職的同時，可報考國營事業考試，善用重疊考科，一次準備就能多次上榜！

上榜路徑大公開！一年內超過8次上榜機會！

初等考	關務特考	鐵路特考	高普考	調查局特考
1月	4月	6月	7月	8月
●最易上手的公職考試	●考科少於同職等考試	(110年因疫情延至9月) ●佐級錄取率最高	(110年因疫情延至10月) ●主流考試，缺額眾多	(110年因疫情延至10月) ●三等月薪76,000起

地方特考	自來水評價人員	台電考試	中油僱員	國營事業職員級
12月	不定期舉辦	不定期舉辦	不定期舉辦	不定期舉辦
●考科同高普考	●只考選擇題	●考科少、好準備	●只考2科，多為選擇題	●國營退休潮，缺額多，工科類科競爭者少

錄取率高

109年
工科錄取率
最高達19.42%

電力工程	電子工程	機械工程	資訊工程
高考 19.42% 普考 17.33%	高考 9.04% 普考 9.39%	高考 18.27% 普考 13.70%	高考 12.92% 普考 10.47%

【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】

- (一)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。
- (二)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。
- (三)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)。
- (四)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。



為你專屬設計的學習模式， 讓你靈活學習、輕鬆準備！

我們都在 **志光學儒保成** 成功找到工科人的工頂人生

多元學習模式



面授學習

直接，有效

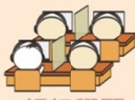
- 實際面對面教學，現場解決您的疑惑。
- 優質專業名師，幫您統整、分析考試重點資訊。
- 定期的大小測驗，您可隨時檢視學習效果。



雲端函授

自主，彈性

- 不用煩惱通勤問題，課程教材直接送到家。
- 反覆聽課，不怕觀念聽不懂。
- 完全自由，可自主安排學習進度。



視訊學習

便利，專注

- 安靜舒適的上課環境，提高您的專注力。
- 看課時間能自由預約，無須擔心時間衝突。
- 可依需求暫停、倒轉或快轉，深度學習超簡單。



專業名師指導，提升解題順暢度！

本以為適合闢蕩，但發現穩定的生活才是我想要的。老師的教材都有明確分析與統整，再加上會由老師出申論題讓考生做練習，增加寫題目的敏感及順暢度。考前還有總複習課程，精準預測範圍、統整考前重點。

全國探花 李○庭 109年鐵路員級機械工程



選對好老師，中年轉職好順利！

我遭遇公司裁員，覺得公職夠穩定，決定踏上國考之路。隔了20幾年重拾書本，選擇好的補習班讓我事半功倍。熱力學老師跟流體力學老師，我非常推崇，只要照著老師講的記下來、寫下來，這樣就夠了。

1年考取 古○芳 109年高考機械工程



題庫班老師的講解，對我幫助很大！

畢業後工作，累的要死薪水卻不怎麼樣。剛好朋友推薦鐵路特考，就挑戰看看。我覺得機械原理的題庫班對我幫助很大，跟著老師一起解，不懂的地方聽老師講解，覺得聽完很多疑問就會解開並且對我幫助很大。

優秀考取 謝○軒 109年鐵路佐級機械工程