第 4 章 資料保護與資訊安全

一 選擇題

(D) 1. 下列哪一項不是個資蒐集者依法要盡到保密及保護的責任？
⑷保持個資的正確性。
⑻告知當事人所蒐集資料的特定目的、使用方式與範圍。
⑹做好安全處理並作適當的刪除與銷毀。
⑽不可刪除與銷毀。

(C) 2. 下列哪一項不是個資法所定義的個資？
⑷姓名、出生年月日、指紋。
⑻婚姻、家庭、教育。
⑹性別、個人興趣、服飾尺寸。
⑽社會活動、聯絡方式、財務狀況。

(C) 3. 下列哪一項不是個資法中的特種個資？
⑷醫療　⑻基因
⑹財務情況　⑽犯罪前科

(D) 4. 下列哪一項不是個資的運用範圍？
⑷蒐集　⑻處理
⑹利用　⑽散布

(A) 5. 網路詐騙案件層出不窮，詐騙手法不斷更新，為確保個資安全，特別要注意自我保護，下列哪一項是不當的措施？
⑷妥善保管自己的個資，但可提供給親友。
⑻在電腦系統完成各項作業後，務必登出帳號。
⑹與他人共用電腦時，切記關閉瀏覽器視窗並清除紀錄，並關掉電源。
⑽儘可能不要使用公共場合中，任何人都能連接上網的無線網路。

(C) 6. 下列哪一項是適當的個人資料保護措施？

(A) 儘量利用公用電腦使用網路服務。

(B) 不要輕易變更密碼。

(C) 勿點選來路不明的網址及程式。

(D) 記錄密碼於電腦或行動裝置內。

(A) 7. 以三層的機制來管理資安的問題，也就是 3A 安全防護，下列哪一項是其合理的順序？

(A) 認證、授權、紀錄。　(B) 認證、紀錄、授權。

(C) 紀錄、認證、授權。　(D) 授權、紀錄、認證。

(A) 8. 關於安裝防毒軟體，下列哪一項不是正確的觀念？

(A) 裝了防毒軟體系統就安全無慮。

(B) 要持續更新防毒軟體才能發揮防毒功效。

(C) 應預約掃描病毒時間，並設定主動掃描檢查，且定期執行。

(D) 避免在使用電腦的工作時間進行掃描病毒。

(D) 9. 下列哪一項可能是釣魚郵件？

(A) 郵件主旨是：更新您的帳戶。

(B) 郵件主旨是：提供帳號密碼以保障您的權益。

(C) 郵件主旨是：提供帳號密碼以確認您的得獎。

(D) 以上皆有可能。

(D) 10. 下列哪一種郵件，最好不要打開，應立即刪除？

(A) 陌生人或非正常的時間寄信。

(B) 主旨過於聳動或看似緊急事情。

(C) 要求提供敏感資料的信件。

(D) 以上皆建議立即刪除。

簡答題

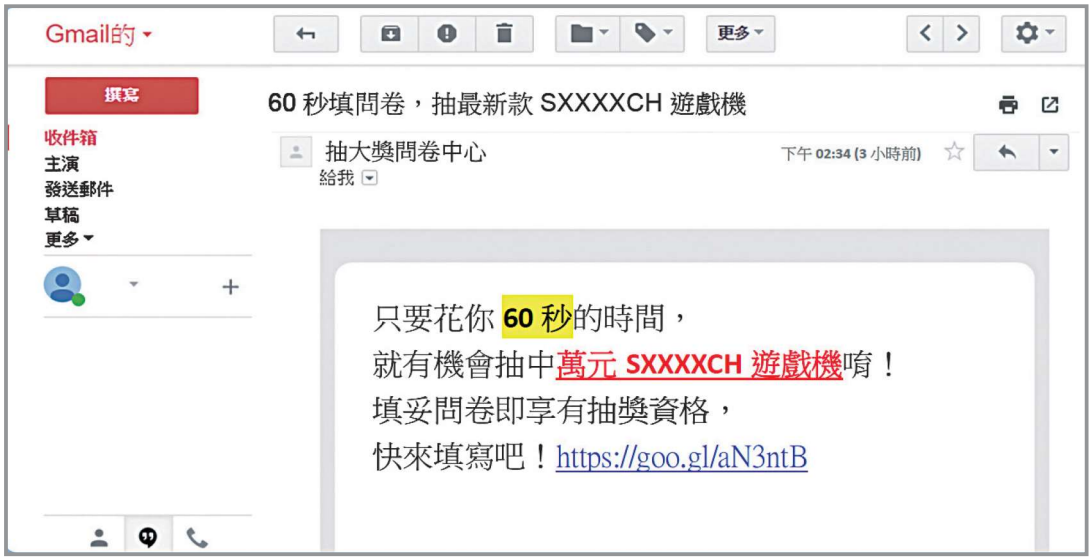
1. 扼要說明什麼是 3A 安全防護？

3A 安全防護是一種內部管理資訊安全的機制，並包含認證、授權、紀錄三層。
第一層是認證，使用者要透過系統認證才能進入系統，並且有使用者身分紀錄。
第二層是授權，透過管理不同使用者有不同的權限，以使用特定資源。
第三層是紀錄，所有使用者使用系統的紀錄，都會留存。系統若出現異狀，即可從紀錄中去查對。

2. 扼要說明什麼是 4D 防護管理？

4D 防護管理是一種防止外部入侵資訊安全的機制，並包含嚇阻、偵測、阻延、禁制四個階段。第一個階段是嚇阻，使入侵者感到被發現的風險高而取消入侵行為。第二個階段是偵測，當被入侵時能即時發現。第三個階段是阻延，使用一些防禦措施，拖延入侵者時間與精力，增加入侵者被發現的機會。第四個階段是禁制，阻止入侵行為，使其無法再侵入。

3. 請問下圖為釣魚郵件或社交工程攻擊郵件？並扼要說明你如何判斷。



(1) 社交工程攻擊
(2) 因為使用人性弱點，以抽大獎的名義引誘收件人為抽獎提供個資，因此判斷其為社交工程攻擊。而且信件標題與內容皆標示不明（如：SXXXXCH 想讓人聯想到 SWITCH，但字數又不符）且聳動，亦未說明活動相關訊息（抽獎程序、領獎辦法、活動時間等）；寄件者也不明（僅有籠統名稱，無人名或公司名）。

討論題

組別 第 4 組 ，共 4 人

組員 陳小翰、林小華、郭小書、李小美

報告方式 ☑海報 ☐簡報 ☐其他：

1. 個人資料保護法定義的個人資料，除了列舉式的項目外，另有一項為：其他得以間接或直接識別該個人的資料。

⑴請問這一項代表什麼意思？

屬於「個人資料」的資料並不是只有個資法所定義的十多項，因無法盡列，所以才有其他得以間接或直接識別該個人的資料這一項。

⑵請問有哪些資料可能可以辨識出某一個「個人」？

a. 相關網路類：我們每天都在使用的網際網路，其中除了 IP 位址外，如 email 位址、Domain Name、URL 位址、Username、以及 Password 等，都是足以識別該個人的資料。

b. 證件類：學生證、健保卡、駕駛執照等。

c. 公家機關資料類：戶口名簿、報稅資料等。

還有很多資料可以辨識個人，無法在此盡列。總而言之，只要可以識別個人身分的資料，都要妥善保管、保密。

2. 依個資法特種個資之保護規定，有關病歷、醫療、基因及健康檢查之個人資料，不得蒐集、處理或利用。但有特殊情況者，不在此限，例如：公立學校基於醫療或衛生之目的，為統計或學術研究而有必要，得蒐集、處理上列特種個人資料，但處理後的揭露方式（如撰寫研究報告或學術研討會口頭報告），蒐集者要注意如何呈現？

處理後的揭露方式，如撰寫研究報告或學術研討會口頭報告等，一定要去個人化，也就是所呈現的資料，不能夠可以識別某一特定的個人。

3. 個人維護資安的意識非常重要，根據你自己的經驗，你是否有過因為不小心而洩露了自己的個資？或是察覺有人想要取得你的個資？如有上列情形，應該要如何處理才妥當？

(1) 如果不小心洩漏了自己的個資，可能會惹來麻煩，因此要小心處理。

a. 若有人試圖跟你連絡（如電話、電子郵件或寫信），建議不要理會，也不要回應。

b. 如果接到陌生人電話，可直接回應：「你打錯了。」，並掛掉電話。

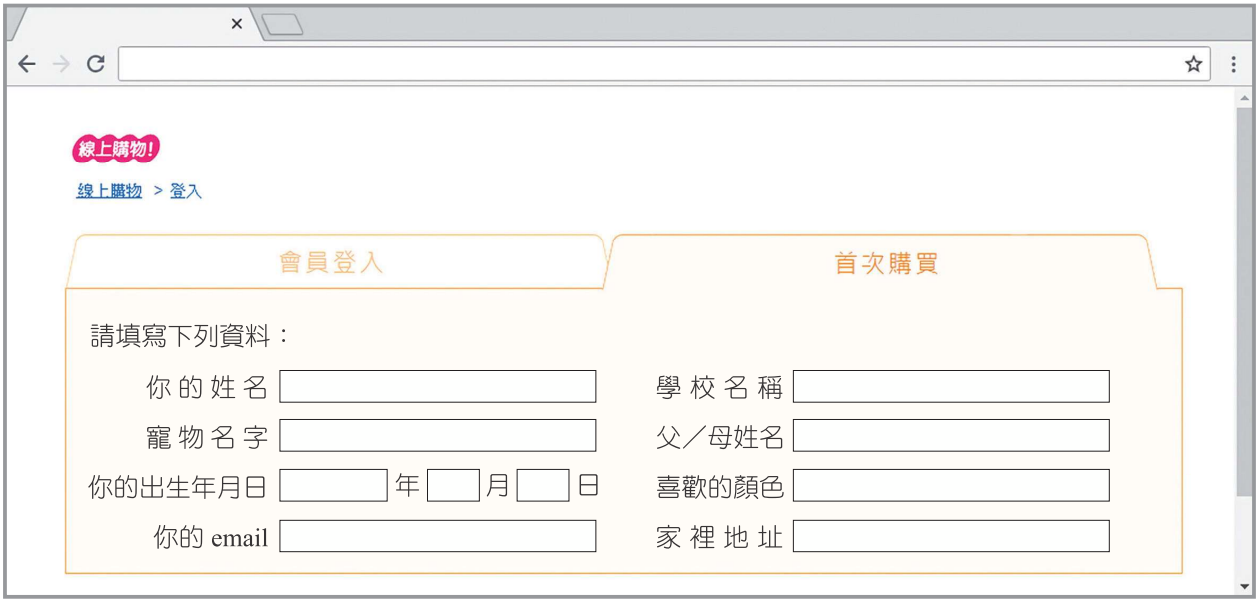
c. 如果有人對你威嚇或分開散布你的部分個資，應即刻報警處理。

(2) 如果發覺有人想取得你的個資，除了小心不要外漏，也要注意其他的防護。

a. 不要貪小便宜，以免因小失大。

b. 應用課本所提供的防護措施判斷郵件，如釣魚網站、社交工程的攻擊、可疑信件等。

4. 某購物網站的畫面如下：



(1) 如果只能填寫其中一部分的資料，而這些資料絕不可以洩漏身分，你認為哪些資料是可以填寫的呢？

a. 寵物名字

b. 學校名稱

c. 喜歡的顏色

(2) 請各組員分享自己所認為可填寫的資料及原因，是否與你所選的相同？

☑是，這些資料中我覺得最不易洩漏身分的資料為 喜歡的顏色 ，

原因：因為顏色有很多種，名稱卻又很統一，因此更不容易從喜歡的顏色辨識出個人 。

☐否，與我所選不同的可填寫資料為 ＿＿＿＿＿＿ ，

原因：＿＿＿＿＿＿ 。

四 案例與分析

【以下引用法條的條項僅供參考依據，不列入學生作答範圍】

組別 第 5 組，共 4 人

組員 林小明、陳小玲、葉小靜、李小強

報告方式 □海報 ☑簡報 □其他：

某大學生星兒利用暑假時應徵到一所私立高中工讀，校長指派她在該校資訊中心盤點應屆畢業生的學籍資料。工作不久後，有一補習班負責人透過星兒的友人傳了訊息給她，請她提供學生的部分資料（如姓名、通信地址及電子郵件等），每位以新台幣十元為報酬，星兒也應允提供。

以上案例，依據個人資料保護法的規定：

1.如果經人告發，星兒要負什麼法律責任？

⑴ 學生個人的學籍資料是屬於個資法的保護範圍。星兒因為未獲得當事人同意或依據其他法定的合法事由就提供個資給他人，屬於個資法中所規定的對個人資料之不當利用，確實侵害當事人權益。

⑵ 依民法第 188 條規定，受僱人因執行職務，不法侵害他人之權利，則僱用人與受僱人須負連帶損害賠償責任，也就是學校與星兒都要負起民事賠償的連帶責任。

2. 校長連帶要負什麼法律責任？

(1) 該學校校長是學校負責人，由於對學生個人資料的保護措施，未盡到注意之職責，因此違反電腦處理個資法第 23 條中個人資料的利用範圍之規範。

(2) 依個資法第 38 條規定，將會遭其目的事業主管機關（教育部），處該校負責人新臺幣二萬元以上～十萬元以下之罰鍰。

(3) 依民法第 188 條規定，受僱人因執行職務，不法侵害他人之權利，則僱用人與受僱人須負連帶損害賠償責任，也就是學校需負起民事賠償的連帶責任。

3. 補習班負責人連帶要負什麼法律責任？

如學校提出告訴，補習班負責人將會觸犯刑法第 359 條之 1 規定，無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。