**數位身分識別管理『解答』**

在所有技術學科中，風險最高的項目為?
a.   網路使用管理
b.√ 身分識別管理
c.   伺服器管理
d.   雲端共享管理

關於「稽核日誌」應保持何種態度面對日誌紀錄?
a.   不理會
b.   隨興
c.√ 理智的
d.   激進的

若欲使用良好的程式碼安全資源，可採用哪一個非營利組織所提供之資源?
a.√ OWASP(開放網路軟體安全計畫)
b.   WTO(世界貿易組織)
c.   WHO(世界衛生組織)
d.   UN(聯合國)

若欲使用「數位簽章」來驗證資料的完整性，又考量成本費用問題，可使用?
a.   騎縫章
b.√ 雜湊訊息驗證碼(HMAC)
c.   筆跡鑑定

「錯誤回應」是數位身分辨別服務的重要組成部分，因為它會告知使用者問題並提高可用性；然而主從式錯誤回應應該注意哪個事項?
a.√ 只包含最少的資訊量以通知使用者
b.   只包含一半的資訊量以通知使用者
c.   包含最多的資訊量以通知使用者
d.   不提供資訊量給使用者

數位身分識別，通常會呼叫外部資料源，故所有來自外部資料源或由使用者提供的資料，其信賴度?
a.   十分可信
b.√ 不可信賴

數位身分識別平台通常十分複雜，僅依靠跨身分識別生態系統元件之通訊協定的固有安全性是不夠的，底層程式碼必須盡可能的安全。為實踐開發身分識別平台的最佳程式碼的安全，可採行以下哪個措施?
a.   使用防禦性程式設計技術
b.   防止未經驗證的程式碼執行
c.   使用稽核日誌
d.   數位簽章
e.√ 以上皆可

為提高程式碼安全性，應避免允許執行未經驗證的程式碼之函數，例如下列哪個函數?
a.√ eval() 類型函數
b.   f(x)函數
c.   g(x)函數
d.   (4)y(x)函數

針對外部命令字串，最佳的的做法為?
a.   直接接受
b.   自行編改後，不須經過濾器檢查即可接受
c.   直接排外
d.√ 經過濾器檢查在該情境中是否有效且適用後，再決議是否接受(需斷句)

在15種最佳程式碼安全實踐方法中，每一種方法皆十分重要，其中最重要的是?
a.   篩檢
b.   檢查漏洞
c.   韌性
d.√ 跟上新興漏洞的腳步

[駭客任務─手機攻防戰](https://elearn.hrd.gov.tw/info/10029136%22%20%5Co%20%22PSCITECHVIS112100111%20-%20%E9%A7%AD%E5%AE%A2%E4%BB%BB%E5%8B%99%E2%94%80%E6%89%8B%E6%A9%9F%E6%94%BB%E9%98%B2%E6%88%B0%28%E5%8F%A6%E9%96%8B%E6%96%B0%E8%A6%96%E7%AA%97%29%22%20%5Ct%20%22_blank)

|  |
| --- |
|  標準答案 學生答案 |
| **配分：[10.00]** | https://scitechvista.elearn.hrd.gov.tw/theme/default/teach/icon_currect.gif得分： | 1. 全球最大的駭客組織為何？1. 繼承者
2. 破壞者
3. 匿名者
4. 台灣記者
 |   |
| **配分：[10.00]** | https://scitechvista.elearn.hrd.gov.tw/theme/default/teach/icon_currect.gif得分： | 2. 下列何者是白帽駭客的別稱？1. 貴族駭客
2. 道德駭客
3. 特種駭客
4. 中正駭客
 |   |
| **配分：[10.00]** | https://scitechvista.elearn.hrd.gov.tw/theme/default/teach/icon_currect.gif得分： | 3. 白帽駭客不知道網站架構下進行攻擊模擬，屬於何種測試？1. 黑箱
2. 灰箱
3. 紅箱
4. 白箱
 |   |
| **配分：[10.00]** | https://scitechvista.elearn.hrd.gov.tw/theme/default/teach/icon_currect.gif得分： | 4. 匿名者屬於何種駭客種類？1. 黑帽駭客
2. 灰帽駭客
3. 紅帽駭客
4. 白帽駭客
 |   |
| **配分：[10.00]** | https://scitechvista.elearn.hrd.gov.tw/theme/default/teach/icon_currect.gif得分： | 5. 下列何種駭客是唯一可以考駭客證照的駭客種類？1. 黑帽駭客
2. 灰帽駭客
3. 紅帽駭客
4. 白帽駭客
 |   |
| **配分：[10.00]** | https://scitechvista.elearn.hrd.gov.tw/theme/default/teach/icon_currect.gif得分： | 6. 下列哪個品牌的手機，其主要作業系統，與其他三者不同？1. Apple
2. Sony
3. HTC
4. Samsung
 |   |
| **配分：[10.00]** | https://scitechvista.elearn.hrd.gov.tw/theme/default/teach/icon_currect.gif得分： | 7. 匿名者多用何種攻擊方式，癱瘓目標網站？1. 蠕蟲病毒
2. 切電源
3. DDoS
4. 木馬病毒
 |   |
| **配分：[10.00]** | https://scitechvista.elearn.hrd.gov.tw/theme/default/teach/icon_currect.gif得分： | 8. 白帽駭客已知道網站架構下進行攻擊模擬，屬於何種測試？1. 黑箱
2. 灰箱
3. 紅箱
4. 白箱
 |   |
| **配分：[10.00]** | https://scitechvista.elearn.hrd.gov.tw/theme/default/teach/icon_currect.gif得分： | 9. 下列哪種駭客，是幫資安公司進行除錯、抓漏的？1. 黑帽駭客
2. 灰帽駭客
3. 紅帽駭客
4. 白帽駭客
 |   |
| **配分：[10.00]** | https://scitechvista.elearn.hrd.gov.tw/theme/default/teach/icon_currect.gif得分： | 10. 何者不是近年匿名者的攻擊目標之一？1. 紅十字會
2. 兒童色情網站
3. ISIS
4. 舊金山捷運
 |  |

# 『解答』電子郵件安全與社交工程防範

為了減少惡意附件的攻擊，建議以文字瀏覽及取消預覽的方式開啟郵件。
a.√ O
b.   X

偽裝郵件帳號與偽裝寄件者都是電子郵件常見的身分偽造手法。
a.√ O
b.   X

收到電子郵件後，安全性檢視的流程為檢視寄件者→郵件主旨→附加檔案→電話確認。
a.√ O
b.   X

企業應落實資安政策，推行內部資安意識的教育訓練，以減少駭客入侵機會。
a.√ O
b.   X

引人注目的電子郵件標題可能是隱藏惡意連結的陷阱，因此要小心謹慎的確認後再開啟。
a.√ O
b.   X

使用任何電子郵件軟體前，先進行確認，是屬於「使用者防護停看聽」的「停」階段。
a.√ O
b.   X

若使用太簡易的密碼很容易被駭客破解，建議同時混用數字、字母及特殊符號來增加困難度，並經常更換帳號密碼。
a.√ O
b.   X

PDF檔無法作為惡意附件的攻擊形式，因此可以放心瀏覽。
a.   O
b.√ X

使用電子郵件時，須確認寄件者與你業務相關且熟識，也要確認電子郵件信箱位址無誤，但不建議關閉郵件預覽功能。
a.   O
b.√ X

詐騙者自稱高階主管、律師要求被害人處理機密性事務，甚至要求匯款至他們所控制的帳戶，此行為是屬於電腦蠕蟲的社交工程術。
a.   O
b.√ X

下列何者非預防變臉詐騙術的防範方式？
a.   加強公司所有個人電腦掃毒
b.   使用合法授權之防毒軟體
c.√ 訂單或出貨單等附件不以加密方式處理
d.   區分管理權限，進行帳號密碼管制

下列何者可能是惡意程式隱藏在電子郵件中的手法呢？
a.   將惡意程式植入解壓縮檔案中
b.   將惡意程式植入附件中
c.   在圖片連結中隱藏惡意程式
d.√ 以上皆是

下列哪一項為社交工程術的非技術性攻擊手法？
a.   跳出的視窗
b.   有趣的軟體
c.√ 假扮技術專家
d.   網路釣魚

下列何者非「使用者防護停看聽」中「看」階段的行為？
a.   確認往來對象
b.√ 透過電話或電子郵件向寄件人確認郵件真偽
c.   可疑主旨勿開啟
d.   可疑檔名勿開啟

下列何者非網路釣魚使用的手法？
a.√ 假貸款真詐騙
b.   建立一個聳動的主旨
c.   常有跳窗網頁
d.   偽造一個相似的網址

下列何者非使用電子郵件前，必須進行的確認行為？
a.   取消信件預覽功能
b.√ 取消純文字瀏覽功能
c.   設定垃圾郵件機制
d.   確認已安裝正版防毒軟體

下列何者為常被用來實施社交攻擊手法的工具？
a.   電子郵件詐騙
b.   線上聊天工具
c.   網路釣魚
d.√ 以上皆是

下列何為內政部刑事警察局教大家的「防騙七招」呢？
a.   定期更新密碼
b.   附件請加密處理，防止資料遭到竄改或偽冒
c.   使用電子憑證以加強驗證
d.√ 以上皆是

我們要如何利用最簡單的方法得知信件中有內崁惡意連結？
a.√ 顯示URL網址來確認
b.   利用防毒軟體確認
c.   確定收件人是否有誤
d.   以上皆是

關於BEC保持安全的提示，下列何者非正確的做法？
a.   仔細檢查所有電子郵件，包括高階主管也是
b.   對員工進行社交工程防範之課程訓練
c.   瞭解客戶的習性，包括交易細節和付款背後的原因
d.√ 供應商付款位置改變由連絡窗口負責認證即可