下列何者通常用於保護傳輸中的數據?

A AES

B Telnet

C TLS (O)

D UDP

吳小姐找來20名友人在網路上團購，個資被盜用，其中6名友人收到「海關公文」，被指控走私電子菸彈。目前海外購物已使用貨物實名制，進出貨都得透過當事人APP「確認」後，才能進到倉儲，為了更加提高資訊安全，減少類似事件，你認為以下何者敘述為非？

A 貨運公司運送貨物作業電子化(O)

B 加強全民資安宣導

C APP確認動作採多階段認證

D 避免網路購物

在傳統網路安全架構設計當中，位於內部的使用者與應用系統，普遍被視為可信任的狀態，因此，較少實施驗證和檢核機制。然而，時至今日，使用者與應用系統執行的位置遍及各處，甚至已經沒有內外之分，此時，我們看待資安防護時，應該採取持續驗證、不輕易信任的態度。零信任模式對於網路流量分析與透視，特別定義出應具備的特性，下列何者不屬於其定義的特性？

A網路鑑識

B封包阻擋(O)

C網路探查

D流向資料分析

墨西哥廠被駭遭勒索 10 億贖金，鴻海：已提高資安層級!

鴻海墨西哥廠在 2005 年時啟用，並將其作為組裝及對美洲出貨電子設備的據點。而根據外國資安網站 Bleeping Computer 報導，此一攻擊是由駭客組織 DoppelPaymer 發起的攻擊，時間點約在 2020年11 月 29 日。

報導中指出，DoppelPaymer 駭客入侵了鴻海北美廠區約 1,200 台伺服器，並竊取了當中 100 GB 的未加密文件、刪除了 20-30TB 的備份資料，以及加密了鴻海相關的文件等。要求鴻海需支付 1,804 枚比特幣（目前市價約 3,450 萬美元）的贖金，才能取得解密工具。

上述資安事件，若您是資安/資訊系統管理者，您應採取的最適措施可能是?

A防毒軟體的使用與病毒碼的更新

B完善的資產管理功能

C帳號權限最小化

D關閉遠端桌面功能(O)

SolarWinds Orion供應鏈攻擊事件震驚全美，美國的"網際安全及基礎設施安全局(CISA, Cybersecurity and Infrastructure Security Agency)在2020年11月12日發了一份聲明, 說美國本次選舉是史上最安全的選舉. 結果最近美國的網路基礎設施傳出被植入後門, 嚴重滲透. 不得已在12/13發出緊急命令, 要求:

1. 對系統影像進行鑑識取證, 及分析新使用者, 服務及特權帳號; 分析已存錄的網路流量.

2. 已受影響的部門必須立即切斷SolarWinds設備的網路或關機. 並移除所有被入侵的帳號.

3. 在指定時間內回報CISA是否有出現特定的威脅特徵.

4. 在移除被入侵的帳號後, 須執行CISA指定的工作項目

針對SolarWinds Orion這次事件的影響,您覺得政府應要的事為?

A限制流量

B盤點SolarWinds Orion產品，儘速確認並進行版本更新(O)

C建議企業/公部門檢視帳號密碼原則

D做DDoS演練

一銀ATM遭駭事件:

這是臺灣金融史上第一次，第一次沒有提款卡也能盜領大量現金的犯罪案件，東歐駭客集團暗中駭入臺灣大型銀行的41臺ATM，從倫敦一臺電話錄音伺服器，橫跨1萬公里，遠端遙控北中兩地22家一銀分行的41臺ATM，還派出十多名車手兵分多路，神不知鬼不覺地盜領8,327萬多元。

如果你是資安優等生，如何快速的逮到嫌疑犯，追回贓款?

A調閱監控系統並報警逮捕嫌疑犯(O)

B聽取電話錄音伺服器之內容

C檢查帳號使用登入紀錄

D調閱伺服器連線紀錄

在區塊鏈應用愈趨多元且蓬勃發展下，隨之而來的資安攻擊，也成為開發者需小心慎防的威脅來源。區塊鏈架構分為資料層、點到點網路層（P2P network）、共識層及應用層，請問以下何種不屬於資料層的威脅來源？

A釣魚攻擊

B不安全的網路位址

C惡意軟體

D阻斷服務攻擊(O)

醫療器材設備與行動裝置的搭配，使得這些器材的運用更為便利，但其中潛伏的資安風險也不應輕忽。2020臺灣駭客年會（HITCON）的遠距議程，德國ERNW資安實驗室發表在胰島素泵浦（insulin pump）上發現的漏洞，駭客可從中進行中間人攻擊，呼籲廠商要重視相關弱點。下列何者為常見的中間人攻擊（Man-in-the-Middle Attack）型式？

A欺騙攻擊 (Spoofing Attack)(O)

B後門攻擊 (Backdoor Attack)

C字典攻擊 (Dictionary Attack)

D阻斷服務攻擊(Deny of service)

微軟於去年宣布成功摧毀了 Necurs 殭屍網路，該殭屍網路已感染全球超過 900 萬台電腦，兩個月內產生了380 萬封垃圾郵件。

據外媒報導，這次微軟能夠破獲 Necurs 殭屍網路得益於 35 個國家 / 地區的國際警察和私人科技公司協調行動的結果。

據上述所提及的殭屍網路之特性何者有誤?

A將使用者的檔案資料進行加密(O)

B傳送垃圾郵件

C可將具有漏洞的設備進行入侵控制

D可進行DDoS攻擊

中秋連假前夕傳出104人力銀行遭中國駭客入侵的消息，高達592萬筆個資盜走，以下何者不是企業網路遭侵入的常見原因？

A Web系統設計的缺陷

B 設備系統老舊(O)

C 系統管理者帳號遭奪權

D 網路防禦機制的漏洞

根據2017年對ZigBee控制智慧燈泡安全性的一項分析顯示，研究人員能夠控制連網Hue燈泡，安裝惡意韌體進而傳播至相近智慧燈泡網路。利用這一遺留漏洞，Check Point更進一步使用 Hue 燈泡作為平台來接管燈泡的橋接器，最終攻擊目標的電腦網路。目前新一代 Hue 燈泡現已修復此漏洞。

攻擊場景如下：

1. 攻擊者控制燈泡的顏色或亮度，讓使用者誤以為燈泡出現故障。該燈泡在使用者的App中顯示為「無法連接」，讓使用者嘗試對其進行「重置」。
2. 重置燈泡的唯一方法是將它從App中刪除，然後命令橋接器重新連接燈泡。
3. 橋接器連接受攻擊的燈泡，使用者將其重新新增到網路中。
4. 攻擊者控制裝有更新韌體的燈泡並使用 ZigBee 協定漏洞向橋接器發送大量資料，以觸發堆積緩衝區溢位（heap-based buffer overflow）。此外，這些資料還允許攻擊者在橋接器上安裝惡意韌體，進而連接到目標企業或家庭網路。
5. 惡意韌體連接回攻擊者，並借助已知漏洞（如 EternalBlue永恆之藍），透過橋接器侵入目標 IP 網路，傳播勒索軟體或間諜軟體。

請問何種方式不能避免類似情況發生？

A 啟動防火牆

B 更新官方韌體

C 安裝第三方韌體(O)

D 安裝防毒軟體

見到QR Code就掃描 二維條碼恐隱藏資安風險

以下敘述何者為非?

A 若見到實體QR Code上有不明黑點，需注意可能為有心人刻意修改內容資訊(O)

B 不只是英數字，就連漢字、符號等都能編碼成QR Code

C QR Code的製作非常容易，任何人都可以利用網路所提供的QR Code產生器

D QR Code隨著不同的版本，可以儲存的資料量也不同

冠狀病毒（COVID 19，俗稱武漢肺炎）侵襲全球滿一年，各方政府企業極力投入的疫苗研發， IBM發布報告警示，駭客們已經盯上了運輸疫苗極為關鍵的「冷鏈」系統。疫苗對運輸環境的嚴苛要求，也導致各個冷鏈公司成為駭客的下手目標。IBM資安研究團隊Security X-Force在一份報告中提到，從去年9月開始，他們發現駭客已在全球六個國家地區中，針對冷鏈設備優化平台（CCEOP）相關組織展開攻勢，且是有高度計畫的行動。  
駭客在偽裝成中國海爾生物醫療（Haier Biomedical）公司的報價信件，並暗藏要求對方輸入資料的惡意網址。IBM認為這次釣魚信件只是攻擊準備，駭客期望藉此收集與運輸疫苗有關的敏感資訊，只要駭客中斷整個疫苗供應鏈中一間公司的付款流程，就可能深深影響疫苗分派。

社交工程演練，為防範網路釣魚信件攻擊的方式之一，請問關於社交工程演練，下列何者為非?

A 以時事或吸引人的標題及內容，制定信件範本

B 於特定時間範圍內，發信給受試者

C 利用電子郵件將惡意程式植入附件檔案中(O)

D 釣魚信件攻擊演練的目的是希望使用者可以了解駭客攻擊的樣態，避免遭受到攻擊。

2020年6月底，資安業者Palo Alto修補藏匿在防火牆作業系統PAN-OS中的CVE-2020-2021漏洞後，7月8日再度修補另一個漏洞CVE-2020-2034。這項漏洞允許未經授權的駭客，以最高權限執行作業系統命令。請問下列哪些不是網路防火牆（Firewall）所提供的功能？

A 網路連線管理稽核

B 阻絕異常存取

C 集中安全控管

D 病毒偵測(O)

在一間咖啡廳喝下午茶發現行動網路訊號較差，便連上咖啡廳的Wi-Fi來上網，請問可能會發生哪種常見的網路攻擊？

A 中間人攻擊(O)

B XSS Injection

C SQL Injection

D 阻斷服務攻擊

Tina 正在為公司規劃新的門禁系統，為了增加安全性，考慮使用生物識別來驗證身份，以視網膜掃描可能會存在什麼問題？

A 視網膜掃描可以洩露個人醫療資訊(O)

B 視網膜掃描儀假陽率較高

C 視網膜掃描可能有害健康，因為需要對著用戶的眼睛噴氣

D 視網膜掃描是最昂貴的生物測定儀器

下列何者不是滲透測試可能的風險？

A 服務終止

B 漏洞利用(O)

C 資料庫數據竄改

D 應用程序錯誤

去年12月初FireEye公布網路遭國家支持的駭客組織駭入，駭客竊取了該公司模擬網路攻擊用以測試客戶環境的\_\_\_\_測試工具。另一方面，FireEye也證實內部網路發現SolarWinds公司遭植入後門程式Sunburst的Orion軟體。請問空白處填入的是？

A白隊

B綠隊

C黑隊

D紅隊(O)

2020年4月，資安廠商發現利用微軟遠端桌面應用程式之DLL Side Loading漏洞，可讓駭客執行遠端程式碼。

請問此漏洞中應用程式搜尋並載入DLL之可能搜尋位置，下列何者為非?

A Windows目錄

B 系統目錄

C 環境變數PATH 中列出的目錄

D 未載入記憶體之任意模組名之DLL (O)

Google Doc 等13 個合法表單服務網站被惡意建立釣魚表單

許多釣魚網頁會放在使用欺騙性網域名稱的網站或用網站產生器製作的網頁。然而最近因為有了僅需幾分鐘即可設定好的工具表單，讓製作釣魚網頁的難度大大降低。

表單產生器之所以成為網路犯罪分子的首選，以下何者為非?

A建立釣魚網頁所需的時間通常很少

B大多的網路表單預設會顯示來源服務商(如Google)的名稱，故讓人降低提防(O)

C可以建立大量的網路釣魚表單

D只需掌握製作表單的基本知識

Google Chrome逐漸採取封鎖HTTP網頁內容的行動，2020年2月Google預告從10月的Chrome 86起完全封鎖不安全的混合內容，也宣佈，將對於以HTTPS網頁中不安全表單傳送資訊發出明顯警告，甚至阻止行動。通訊協定中https使用的是何種加密協定？

A RSA

B ATM

C SET

D SSL (O)

安全研究人員發現Ruckus Wireless中小企業路由器產品三項不同的驗證前(pre-authentication)遠端程式碼執行漏洞，可能讓駭客遠端駭入甚至接管機器。所謂驗證前漏洞即指攻擊者不需密碼即可存取機器，請問何者不是駭客的目的？

A 格式化字串攻擊(format string attack) (O)

B 路徑穿越(path traversal)

C 指令注入

D 堆疊溢位(stack overflow)

2018年1月Coincheck於遭遇駭客攻擊，平台全部（5.26 億個）NEM 幣（新經幣）被非法轉移。根據估算，這批丟失的新經幣價值 5.23 億美金（約為台幣 152 億元），這是歷史上最大規模的數位貨幣盜竊案。請問下列關於數位貨幣的敘述何者正確?

A 數位貨幣很安全未來只會越有價值，這只是交易平台管理上出了疏漏

B 未來量子電腦運算能破解數位貨幣加密演算法，根本是無稽之談

C 區塊鏈把線性鏈組成一個一個區塊，然後為每個區塊算出一個特徵值，最後把這些區塊用他們的特徵值串聯成資料紀錄

D 分散式帳本技術又叫作區塊鏈，來防止已被寫入帳本之虛擬貨幣使用紀錄被惡意竄改(O)

有關風險評鑑循環，請排出順序:

1. 資安風險評鑑之行動
2. 資安風險評鑑之建置與實施
3. 規劃資安風險評鑑
4. 資安風險評鑑之檢查作業

A丙、乙、丁、甲(O)

B甲、乙、丙、丁

C丁、丙、乙、甲

D丙、甲、乙、丁

Ryan是MMS系統的安全管理人員。針對新員工建立帳號時，應該給予所有新員工什麼預設訪問權限?

A管理員

B無訪問(O)

C只讀

D編輯

網際網路安全協定（Internet Protocol Security，縮寫：IPsec）是一個協定套件，透過對IP協定的封包進行加密和認證來保護IP協定的網路傳輸協定集合。由三個主要協定組成，下列何者協定不在此集合內？

A網際網路金鑰交換（Internet Key Exchange，IKE）

B認證頭（Authentication Header，AH）

C封裝安全載荷（Encapsulating Security Payload，ESP）

D可延伸訊息與存在協定（Extensible Messaging and Presence Protocol，XMPP）(O)

在資料進行傳輸過程中所使用的加密協定，下列何者為目前最安全者？

A DES

B TLS 1.2(O)

C AES

D SSL 3.0

年度電玩遊戲大作(Cyberpunk 2077)上市5天後，有資安研究員發現，駭客竟以提供Windows和Android測試版遊戲的名義，佯稱提供玩家免費下載，但他們提供的安裝檔案，實際上是勒索軟體CoderWare，在當時65個防毒軟體只有29個判別該檔案為病毒。諸如此類社交工程的資安攻擊，下列何者非防範措施？

A資訊資產分級

B資料備份

C寄信使用密件收件人

D不使用公共 Wi-Fi(O)

在操作系統加載之前，通過更改系統引導過程和重定向BIOS來加載惡意軟體，哪種類型的病毒會這樣執行?

A 服務注入

B 隨機加密

C MBR(Master Boot Record主開機記錄)(O)

D 文件感染

美國聯邦調查局（FBI） 日前發表資安通報，指出有愈來愈多駭侵團體，最近開始針對 Web Mail 服務自動轉寄的郵件規則發動 BEC（Business Email Compromise） 攻擊，來盜領企業的各種帳款，造成極大損失。

FBI 指出，在疫情影響之下，愈來愈多中小企業採用遠距工作，並且更為依賴以網頁為基礎的 Web Mail 服務，較少使用本機的郵件軟體收發信件。

以下何者不是避免電子郵件社交工程攻擊的做法?

A安裝防毒軟體，確實更新病毒碼

B以電話確認電子信件是否來自平時來往的部門單位

C制定企業資訊安全政策，禁止使用非法郵件軟體(O)

D取消信件預覽功能

硬體加密貨幣錢包製造商Ledger於去年7月遭到駭客入侵，當時Ledger聘請了外部的鑑識專家，判斷有9,500名用戶的個資外洩。  
根據Ledger最新的調查，駭客在去年7月入侵了該平臺的行銷與電子商務資料庫，存取了約100萬名訂閱電子報的用戶電子郵件帳號，更嚴重的是，駭客也存取了27.2萬名訂閱了Ledger服務的用戶資料，包括他們的電子郵件帳號、姓名、電話號碼、地址，以及所購買的產品類別。  
Ledger的主力商品為加密貨幣硬體錢包，可用來存放、管理與銷售加密貨幣，由於它平常並未連上網路，因此又被稱為冷錢包，透過由24個單字所產生的恢復碼（Recovery Phrase）進行保護，亦可添增短語密碼。  
如果您是 Ledger使用者，你不該做以下哪件事？

A立刻修改Ledger平台密碼

B打電話到 Ledger客服詢問如何處理此次駭客事件

C因為對此事件有疑慮，所以先暫停 Ledger的使用

D開啟一封疑似來自於 Ledger工程部的信，信中指示你提供恢復碼，以便幫你恢復服務(O)

2020年SolarWinds產品在美國遭受駭客滲透的相關APT攻擊，已對各級政府組織、重大基礎設施，以及私人組織帶來威脅。請問如果民眾連結到這些網站，下列敘述何者正確?

A只要沒有輸入個人資料，就安全無虞

B只要電腦有安裝防毒軟體與防火牆，就安全無虞

C民眾的個人資料可能被竊取(O)

D個人資料不重要，不需要擔心被竊取