【行動支付安全】解答

手機被盜時，所有行動支付損失一概由消費者負擔。
a. O
b.√ X

市面上的行動支付方式非常多，消費者只要選擇其中一樣即可在台灣暢行無阻。
a. O
b.√ X

行動支付的優點有哪些？
a.√ 只帶手機出門即可輕鬆支付
b. 使用時一定會有消費折扣與紅利點數回饋
c.√ 可讓消費紀錄一目了然
d.√ 若結合雲端發票，可讓對獎更容易也更環保

使用條碼支付有何好處？
a.√ 店家不用準備 POS 機
b.√ 只需要一個 App 就能收帳
c.√ 較不會有手機型號上的限制
d. 機若具備 NFC 功能支付會更迅速

不僅可從事代收代付業務，帳戶也有儲值、轉帳等功能的，是屬於哪一種行動支付的營業模式？
a.√ 電子支付
b. 電子票證
c. 第三方支付

Apple Pay、Google Pay 與 Samsung Pay 採用的是何種交易模式？
a.√ 感應支付
b. 條碼支付
c. 現金支付
d. 紅利點數支付

不可儲值也不可轉帳，並由信用卡收單機構簽訂「提供網路交易代收代付服務平台業者」為特約商店等自律規範，指的是下列何者？
a. 電子支付
b. 電子票證
c.√ 第三方支付

當接到銀行電話詢問存款帳號、身分證字號等資料時，我們應該怎麼做？
a. 配合提供相關資料
b.√ 與銀行客服專線確認
c.√ 撥打 165 警政專線求證通報

行動支付綁定的信用卡不小心遭盜刷時，以下處理程序何者正確？
a. 簽「爭議帳款聲明書」→報警備案→打給銀行客服掛失卡片
b. 打給銀行客服掛失卡片→報警備案→簽「爭議帳款聲明書」
c.√ 打給銀行客服掛失卡片→簽「爭議帳款聲明書」→報警備案
d. 報警備案→簽「爭議帳款聲明書」→打給銀行客服掛失卡片

信用卡號代碼化，交易時不會記錄信用卡號碼，信用卡資訊也不會保存在店家與設備內，指的是什麼？

a. Near Field Communication
b. Mobile Payment
c. Secure Element
d.√ Tokenization

以下哪些方法可以降低駭客透過讓受害者掃描假的 QR Code 或開啟偽冒的釣魚網址，進而控制受害者帳戶竊取登入資訊進行盜刷的風險？

a.√ 針對可疑的連結提高警覺
b.√ 儘速套用安全更新
c. 避免更新手機裡的 App 軟體
d.√ 只從官方應用程式商店下載程式

關於條碼支付，下列敘述何者正確？

a.√ LINE Pay、街口支付皆屬之
b. 出示給商家掃描的 QR Code 可截圖後重複使用
c.√ 比起感應支付較不會有智慧型手機型號的限制
d. 使用的商家須購買 POS 機

下列哪些行動支付的操作方式為在 POS 機「嗶」一下即可？

a. LINE Pay
b. 街口支付
c.√ Apple Pay
d.√ Google Pay

哪種支付方式主要開放簽帳金融卡綁定，可支援 NFC 感應支付與條碼支付，只要掃描帳單上的 QRcode 就可直接繳水電等公共事業費？

a. LINE Pay
b. 街口支付
c.√ 台灣 Pay
d. Google Pay

下列何者非取得電子票證執照的業者可以從事的行為？

a. 代收款項
b. 代付款項
c. 儲值金錢
d.√ 轉帳

【物聯網安全概論】解答

物聯網裝置需於開機時就檢查韌體及系統軟體的數位簽章或摘要值，確保只會載入原始軟體，防止遭駭客植入惡意程式而破壞系統的完整性，請問這項功能為何?

a. 韌體自動更新
b.√ 安全啟動設計
c. 完整性檢查功能
d. 數位簽署能力

下列哪一項物聯網裝置的安全性功能最能夠有效降低弱點被駭客利用的風險?

a. 允許變更為複雜密碼
b.√ 即時更新功能
c. 支援事件記錄功能
d. 安全性啟動功能

下列何者並非物聯網的三層式架構層次?

a. 感知層
b.√ 雲端層
c. 網路層
d. 應用層

物聯網系統的安全性保護工作需先確保重要資料不會外洩，請問這需要提供哪一項安全性服務?

a. 可用性 (Availability)
b. 完整性 (Integrity)
c.√ 機密性 (Confidentiality)
d. 身分驗證 (Authentication)

許多物聯網裝置大多因缺乏何種能力而導致一旦被發現漏洞，將持續存在被利用攻擊的風險?

a. 預設帳戶密碼無法修改
b.√ 韌體更新機制
c. 無法整合或相容於現代防火牆
d. 無法執行弱點掃描

下列有關於物聯網安全性問題與挑戰的相關描述，何者有誤?

a. 物聯網系統的安全性責任歸屬，非屬單方面責任
b. 安全性設計不良與不足的物聯網裝置上市，將使全球網路攻擊的可行性和機率提升
c. 目前許多物聯網系統較缺乏軟硬體更新機制
d.√ 物聯網系統的連網性和智慧功能讓它難以做安全性評估與防範

下列哪一項技術並無法設計用來區隔物聯網裝置與一般網路裝置?

a. VLAN
b. 多重 SSID
c. 防火牆
d.√ 集線器

物聯網裝置眾多且欠缺安全性功能，因此可能輕易為駭客掌控而組成殭屍網路，進行下列何種攻擊?

a. 連線攔截 (Session Hijacking)

b. 分散式密碼破解 (Distributed Password Cracking)

c.√ 阻斷服務攻擊 (Denial-Of-Service)

d. 社交工程(Social Engineering)

不安全的網頁介面經常是物聯網系統被利用攻擊的主要漏洞，下列何者並非針對此項漏洞的有效因應做法?

a.√ 網頁檔案加密儲存

b. 變更網頁連線的預設帳戶和密碼並且使用複雜密碼

c. 測試並確認可免於 SQL 注入、XSS、CSRF 等攻擊

d. 安全的網頁工作階段管理

許多物聯網裝置採用計算力較低的處理器和低容量的記憶單元，因此無法實現下列哪種功能而導致裝置本身於資料傳輸與儲存時易受攻擊?

a. 更新機制

b. 弱點掃描

c. 防毒功能

d.√ 加密功能

【最佳密碼建議】解答

由於量子電腦的研發越來越快，導致何種加密方式備受重視?

a. 分子密碼學
b.√ 量子密碼學
c. 傳統密碼學
d. 非典型密碼學

為降低駭客破解率，密碼設定最重要的是?

a. 複雜度
b.√ 長度

量子電腦若發展完備，可在幾秒內破解現有公鑰系統密碼，所以當前防禦量子加密的第一道防線為?

a. 更簡單的金鑰
b. 更複雜的金鑰
c.√ 更長的金鑰
d. 更短的金鑰

密碼被攻破的主要原因為何?

a. 密碼猜測
b. 暴力破解
c.√ 以上皆是

加密與解密使用一對金鑰稱為?

a. 對稱式金鑰(私鑰加密)
b.√ 非對稱式金鑰(公鑰加密)
c. 關連式金鑰
d. 非關連式金鑰

現今理論上無法完全破解的技術為何?

a.√ 量子金鑰分發(QKD)
b. 進階加密標準(AES)
c. 美國資料加密標準(DES)
d. 數字簽名演算法(DSA)

密碼管理工具最主要的功能是?

a.√ 創造冗長密碼
b. 創造簡短密碼
c. 增加密碼輸入麻煩
d. 多餘的管理工具

使用密碼保護時，建議的方式?

a. 冗長
b. 勿重複
c. 複雜
d.√ 以上皆是

下列哪些選項受到非對稱式加密(公鑰加密)所保護?

a. 電子郵件
b. 網站
c. 金融交易
d.√ 以上皆是

以下哪個密碼長度較為安全?

a. 3-6 碼
b. 6-9 碼
c. 9-12 碼
d.√ 12-16 碼以上