香港紅卍字會大埔卍慈中學

高中應用學習課程-資訊科技精要
(2023-2025ECC學年）

單元六：數據通知和網絡
課業六：網絡安全認知（移動支付）

第四組組員：
鍾楚真（組長）
黃舜朗
林翼亮
李銘軒

移動支付
的基本概念與應用範圍

移動支付的特點

方便快捷

移動支付可以在任何時間、任何地點完成交易,為用戶帶來極大的便利性。

安全可靠

移動支付採用複雜的身份認證和加密技術,提高了交易的安全性和隱私保護。即使遺失手機,用戶的資金和個人信息也能得到有效保護。

全面普及

隨著智能手機的普及和5G網絡的推廣,移動支付正在快速滲透到社會的各個層面,為生活帶來便利。

創新體驗

移動支付不僅改變了支付方式,為用戶帶來全新的互動體驗。

移動支付的技術特性和運作原理

1 **行動裝置**

以智能手機為主的行動裝置

2 **支付傳輸**

利用無線網路或藍牙技術進行支付交易

3 **安全機制**

採用加密、生物辨識等確保交易安全

移動支付的核心技術包括行動裝置作為支付工具、採用無線網路或藍牙進行交易傳輸、以及加密和生物辨識等先進的支付安全機制。這些技術特性共同構成了移動支付的運作原理,實現了安全、便捷的跨設備行動支付服務。

移動支付的歷史發展和未來趨勢

早期發展

移動支付的概念最早出現於20世紀90年代,當時短信和WAP技術的簡單支付服務開始崛起。

1

2

技術升級

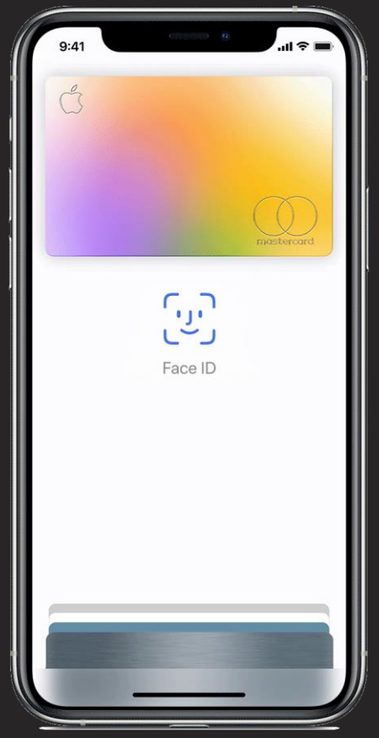
隨著智能手機、NFC(近場通訊)和藍牙等技術的不斷進步,移動支付服務得到了進一步發展和完善。

3

市場普及

移動支付已經從最初的概念演化成為一種廣泛應用的支付方式,深入到日常生活的各個方面。

移動支付的主要優勢和創新點



安全性

移動支付通過加密技術和生物特徵認證,大幅提升了交易的安全性,有效防範了賬戶盜用和詐騙風險。

便利性

移動支付實現了無現金支付和快速結帳,用戶無需攜帶現金或卡片,既節省時間又提高購物體驗。

移動支付的效率、成本、便利性提升具體表現

效率提升

通過移動支付免除了排隊等候的時間,交易能夠快速完成,大幅提高了交易效率。

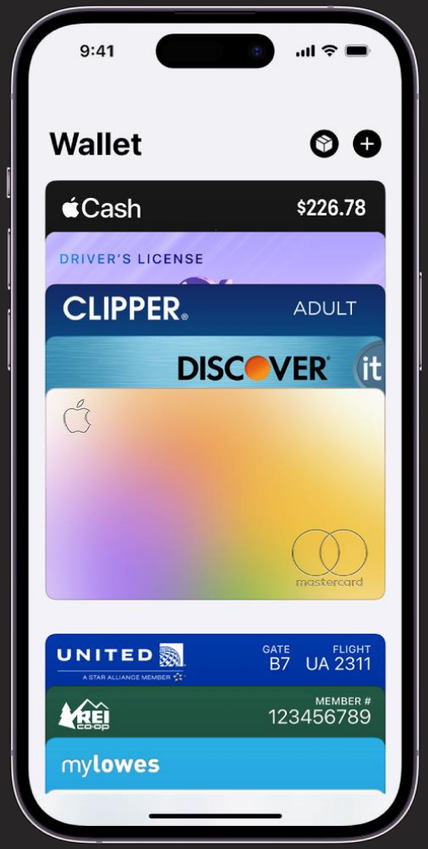
成本降低

移動支付減少了現金和實體卡的使用成本,同時優化了支付和結算流程,降低了整體運營成本。

便利性提升

移動支付只需一部智能手機即可完成支付,大大提高了支付的便捷性和普及度,讓支付變得易捷。

移動支付的具體應用場景或案例



移動支付的應用場景廣泛，包括餐飲、零售、交通、公共服務等多個方面。常見的應用案例有手機支付消費、掃碼支付、線上購物、共享單車等。這些場景都能大幅提升消費者的支付便利性和效率。

移動支付對應用場景中的效益和挑戰

1 **增強效率 ⚡**

移動支付極大降低了支付過程中的時間和精力成本,讓付款交易更加快捷高效。

2 **提升便利性 💪**

用戶只需通過手機就可以完成付款,大幅提升了支付的便利性和用戶體驗。

3 **安全性挑戰 🔒**

確保移動支付交易的隱私性和安全性仍是一大挑戰。

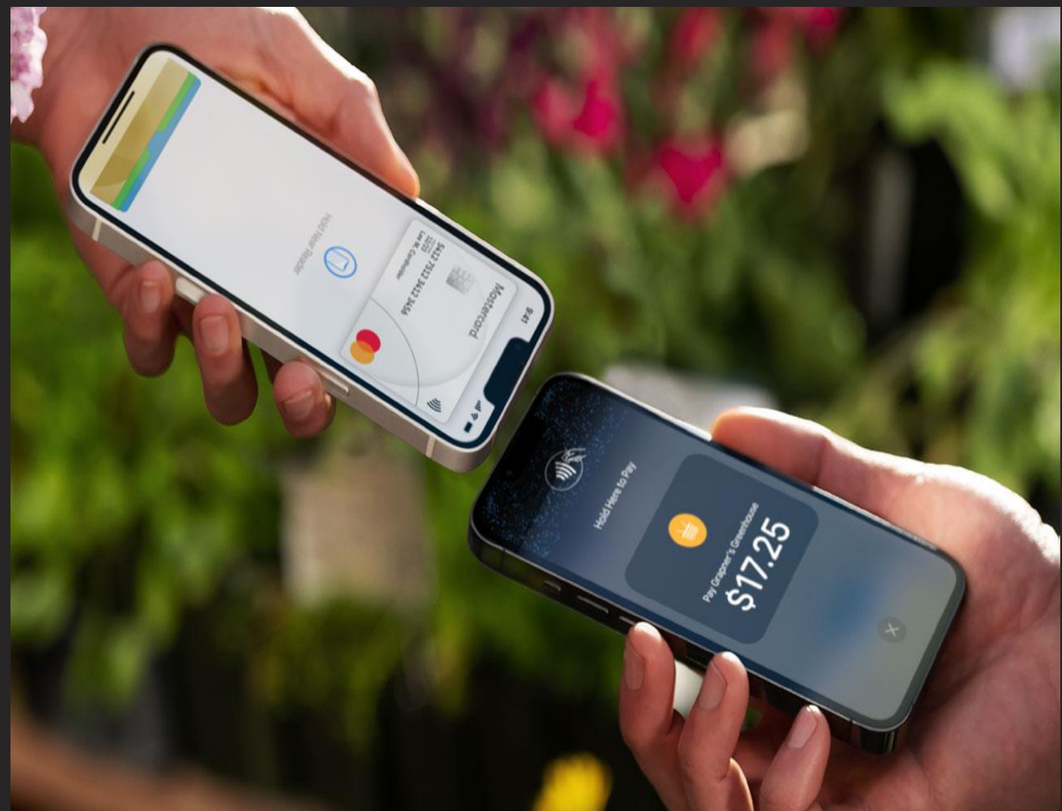
移動支付的效率、成本、便利性提升具體表現

移動支付技術的成熟和普及，大幅提高了支付的效率和便利性。

不再需要攜帶現金和卡片,只需輕點手機即可完成支付,大大簡化了支付流程。

同時,移動支付還降低了商家的收款成本,

提高了交易效率,促進了消費者和商家之間的互動。



移動支付的未來趨勢

隨著技術的不斷進步和消費者需求的不斷變化,移動支付的發展前景廣闊。未來將出現更多創新應用,提升支付效率和便利性。

移動支付威脅分析

威脅分析是評估移動支付系統可能面臨的風險的重要一環。威脅的性質、來源和嚴重程度是十分影響的。

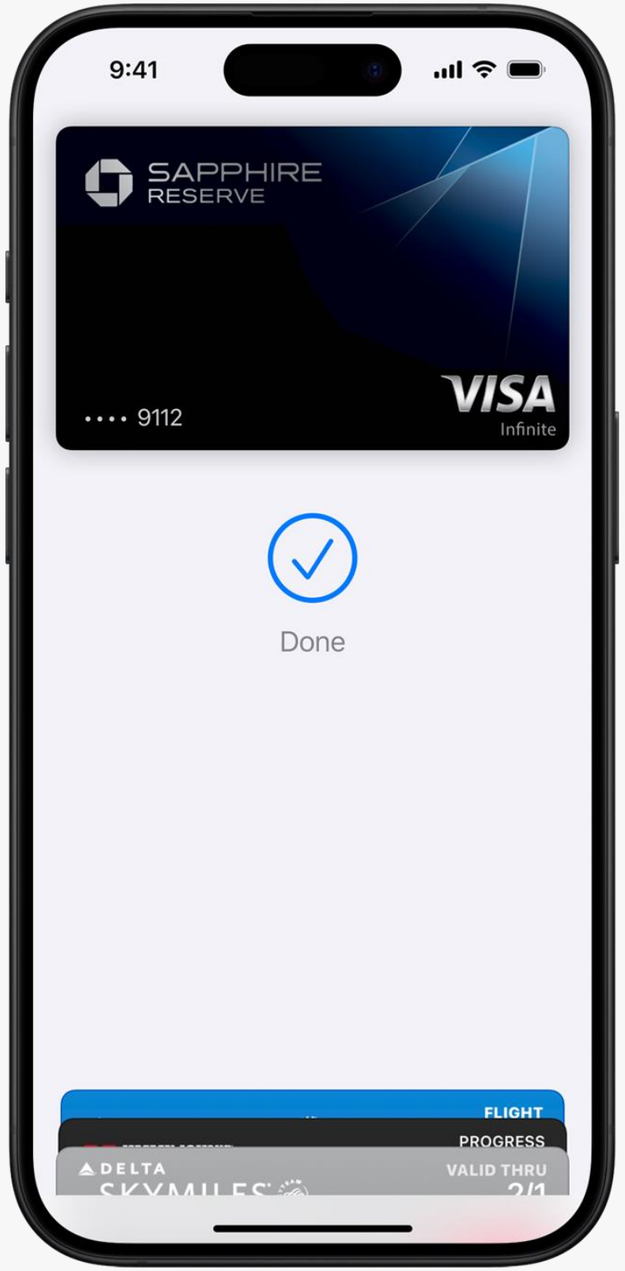
通過了解這些因素，可以制定有效的安全策略，以降低風險並保護用戶的數據和資金安全。

鍾楚真

黃舜朗

林翼亮

李銘軒



威脅分析：評估與對策

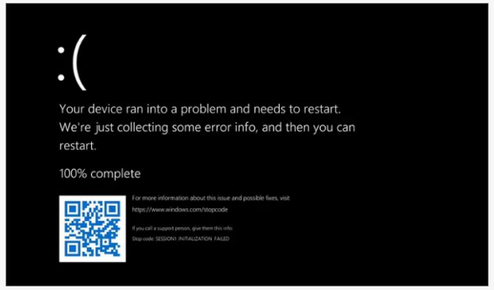
威脅可能性

移動支付的威脅可能性需要綜合評估。常見的威脅來源包括：惡意軟體、釣魚攻擊、資料外洩等。威脅發生的可能性會受到系統安全性、使用者行為、網路環境的影響。

對策

針對移動支付的威脅，需要採取多層次的安全措施。例如，使用多重身份驗證、防病毒軟體、防火牆等。

威脅來源和範疇



硬體故障

硬體故障可能是移動支付系統面臨的重大威脅。伺服器或網路設備的故障可能會導致服務中斷，影響交易的進行。

資料完整性、可用性和機密性

移動支付系統可能面臨資料完整性、可用性和機密性的威脅。

威脅的持續時間與反應策略

威脅持續時間

威脅的持續時間決定了防禦措施的複雜性。短期威脅可以通過快速應急措施解決。長期則需要更多時間或人手處理。

長期威脅的防護

對於長期存在的威脅，應建立強大的安全機制，例如更新防護軟體。

應急計劃

針對每一種威脅，應制定完善的應急計劃，例如系統恢復等方面的步驟。

問題細節和影響分析

1 問題細節

首先要明確問題的具體情況。比如，是系統漏洞導致的攻擊，還是系統配置錯誤導致的數據洩露！了解問題發生的細節對於制定解決方案至關重要。

2 發生過程

接下來，需要了解問題是事件是如何發生的。例如，數據是如何洩露？通過分析問題的發生過程，可以找出漏洞所在，並採取措施防止類似事件再次發生。

3 影響範圍

確定問題影響了哪些部分。是影響了全部系統，還是只影響了部分功能？哪些用戶或客戶受到影響？明確的影響範圍可幫助制定更有效的應對措施。

4 用戶和客戶

具體哪些用戶或客戶受到影響，需要進行詳細調查。例如，數據洩露是否導致用戶信息被盜？這些信息將有助於對評估嚴重程度並制定相應的補救措施。

問題解決與應對

1 數據收集

全面收集並分析相關數據，以深入理解問題的根源和影響。

2 策略制定

根據已知的解決方案或緩解措施，制定一個有效的行動計劃。

3 執行與評估

按照制定的策略執行方案，並定期評估其效果。

通過數據收集，可以更好地了解問題的範圍和影響，並制定更有效的解決策略。

在執行解決方案時，需要密切監控，並根據實際情況做出調整，以確保問題得到徹底解決。

持續監控

設定警報

設定系統警報，以偵測任何異常活動或潛在威脅，例如：異常訪問。

定期審查

定期審查安全日誌尋找任何潛在問題或安全漏洞。

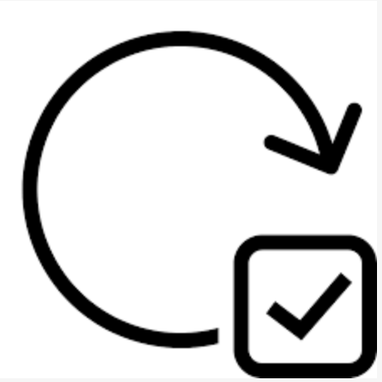
安全評估

定期進行安全評估，以識別潛在的漏洞和風險，并提供改進措施。

真實案例：移動支付安全漏洞

移動支付平台「PayEasy」遭遇大規模數據洩露事件，共影響超過 100 萬名用戶。攻擊者利用平台的 API 漏洞，盜取用戶的支付信息，包括姓名、手機號碼、銀行卡號碼和交易紀錄。此事件暴露了移動支付平台在安全方面存在的嚴重漏洞，凸顯了 API 安全的重要性。

解決方案評估



解決方案描述

該問題透過系統升級、安全漏洞修補。

解決方案效果

經過解決方案實現後，移動支付系統的安全性得到提升，並有效防止了類似問題再次發生。

從案例中學習

經驗教訓

透過案例，學習如何防範移動支付安全威脅。了解漏洞、攻擊手法，提升安全意識。

未來預防

建立嚴謹的防護機制，例如多重驗證、資料加密，定期更新系統。

移動支付的保護措施

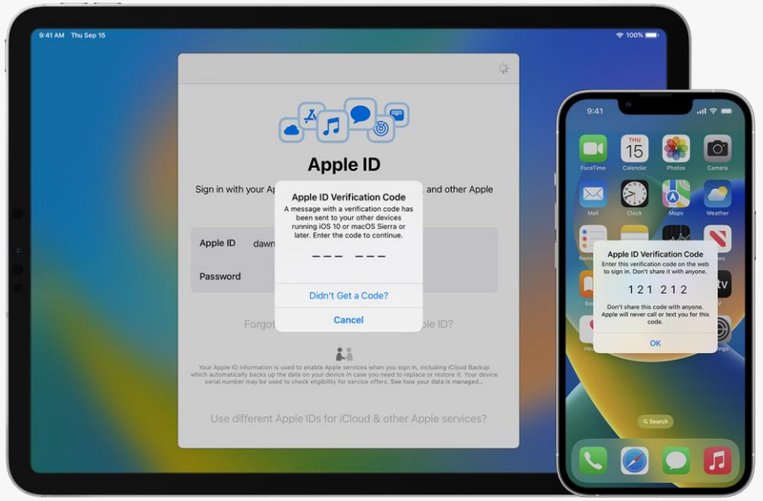
移動支付的普及帶來便利，但也面臨著安全威脅。
該如何有效地保護移動支付系統，抵禦各種威脅，才是關鍵。

鍾楚真
黃舜朗
林翼亮
李銘軒

保護措施

資料加密

資料加密可以保護敏感資訊，例如帳戶資訊和交易紀錄。



雙重驗證

雙重驗證需要使用者進行多個安全認證，例如密碼和行動裝置上的短訊或驗證碼。這是一種簡單且有效的防禦措施。

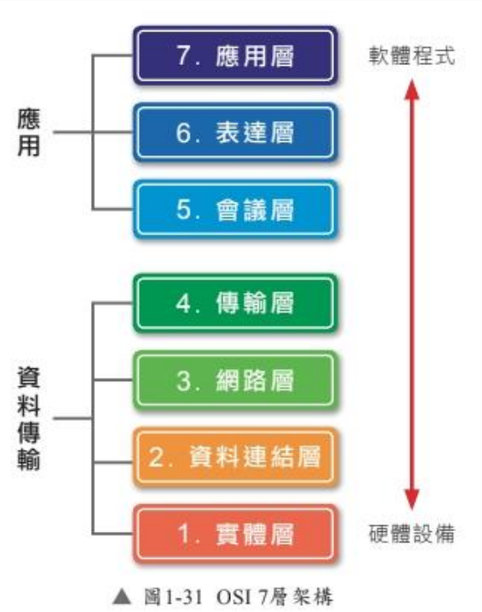
OSI 模型連繫

移動支付系統涉及多個 OSI 模型層，例如應用層、傳輸層、網絡層和數據鏈路層。

1. 應用層
   用戶介面和交易處理
2. 傳輸層
   安全連接和數據傳輸
3. 網絡層
   路由和地址解析
4. 數據鏈路層
   網絡介面卡和網路介面

這些層面都可能受到安全威脅，例如資料竊取或未經授權的訪問。

該問題主要影響哪一層？請詳細說明。



▲ 圖1-31 OSI 7層架構

應用層

移動支付的安全性問題主要影響 OSI 模型的應用層。應用層負責提供用戶界面、應用程序邏輯和數據格式轉換。它直接與用戶交互，因此在處理支付數據、身份驗證和安全協議時，特別容易受到攻擊。

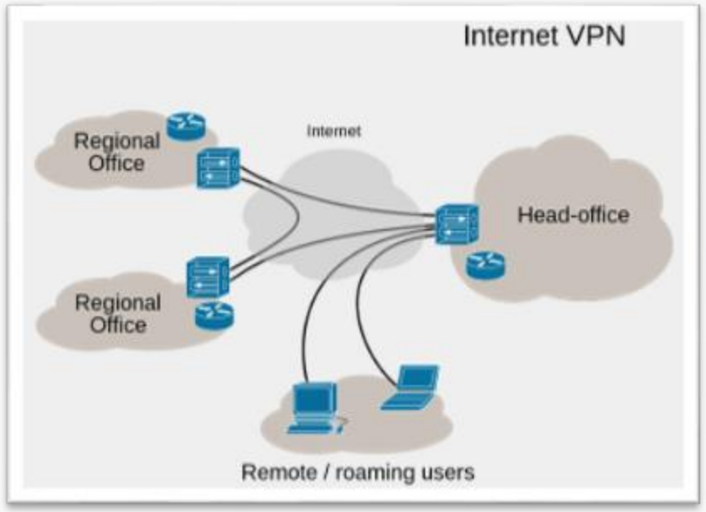
安全性漏洞

在應用層，安全漏洞可能導致數據洩露、欺詐性交易和用戶帳戶盜用。例如，惡意軟件可以竊取支付信息，或攻擊者可以利用應用程序中的漏洞來繞過身份驗證機制。

針對該層的專門防禦措施或技術

防火牆

防火牆是網絡安全的重要組成部分，它們可以阻止來自不受信任網絡的訪問，並防止惡意軟件入侵。



虛擬私人網絡 (VPN)

VPN 可以加密網絡流量，並通過安全隧道將數據傳輸到目的地，從而提高網絡安全性。

TCP/IP 模型連繫

1 應用層

移動支付的安全性主要與應用層相關，例如支付應用程式，以及用戶與服務器之間的通信。

2 傳輸層

移動支付的安全問題也涉及傳輸層，例如確保數據傳輸的完整性和機密性，防止數據被竊取或篡改。

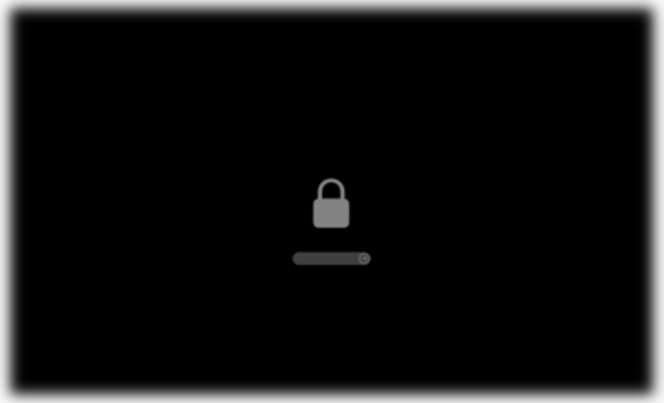
3 網路層

網路層主要負責資料的路由和位址轉換，行動支付安全問題的影響較小，因為網路層更專注於資料傳輸而不是資料內容。

針對該層的專門防禦措施或技術

網路層安全技術

網路層提供資料傳輸功能，可使用防火牆、入侵偵測系統 (IDS) 和入侵防禦系統 (IPS) 監控網路流量，並阻擋或隔離惡意流量。



加密技術

加密技術透過密鑰和演算法，將資料轉換為無法理解的格式，即使資料被竊取，也無法被破解，以保護資料機密性。

網絡架構模型連繫

零信任架構

零信任架構是一種安全模型，假設所有網絡流量都是不可信的，需要通過驗證和授權才能訪問資源。

移動支付安全

移動支付系統在零信任架構下，需要嚴格驗證和授權，防止未經授權的訪問和資料洩露。

影響部分

移動支付的安全問題影響了零信任架構的驗證和授權機制，以及資料加密和傳輸安全。

網絡架構模型連繫：影響部分

1 身份驗證與授權

移動支付系統中，身份驗證與授權是關鍵的防禦措施。攻擊者可能利用弱點，繞過身份驗證，或盜取使用者權限，執行未經授權的交易。

2 設備安全

移動設備本身的安全非常重要，攻擊者可能利用設備漏洞，入侵設備，竊取支付資訊，或執行惡意操作。

針對這些部分的專門防禦措施或技術

資料加密

資料加密是一種保護敏感資料的重要方法，它使用密碼對資料進行編碼，使其在未經授權的情況下無法讀取。

入侵偵測和防禦系統

入侵偵測和防禦系統（IDS/IPS）監控網絡流量以檢測可疑活動並阻止潛在的威脅。

移動支付的跨領域整合與合作

移動支付作為一項嶄新的技術，正不斷與大數據分析、區塊鏈等新興技術進行深度整合，開拓出無數創新的應用場景，為企業和用戶帶來前所未有的便利和機遇。

跨領域整合：開拓無限可能

大數據分析

移動支付系統包含豐富的用戶交易數據，與大數據分析技術的結合，可提供個性化的金融服務和精準的消費紀錄。

區塊鏈

區塊鏈的去中心化特性可確保移動支付交易的安全性和透明度。

物聯網

移動支付可實現設備間的自動化支付。

整合過程中的挑戰

1 技術互通

確保不同系統間的數據交換和流轉,實現無縫銜接。

2 安全性管控

確保數據隱私和交易安全,預防網絡攻擊和欺詐行為。

3 標準制定

制定統一的技術標準和行業規範。

4 法規政策

適應監管環境的變化,確保合規性。

整合案例：智慧城市支付

公共交通

移動支付與NFC技術結合,實現乘車刷卡、自動結算。

停車導航

停車APP與移動支付融合,實現智慧停車管理和無縫支付。

生活服務

移動支付與物聯網深度結合,支持日常生活的各類支付。

成本效益與可行性

成本優勢

無需額外硬件設備投入,可利用有移動設備實現支付功能。

用戶體驗

提升用戶便利性和支付效率。

運營效率

減少人工成本,提高資金流轉速,降低運營風險。

市場潛力

配合多種技術一起運用。

合作機制：推動行業進步

技術聯盟

跨行業企業共同開發標準和技術規範。

校企合作

與高校合作,創新應用和人才培養。

政企合作

與政府部門合作,制定行業政策和監管標準。

投融資合作

吸引各類投資者共同一起合作。

合作中的風險管理

知識產權保護	建立健全的專利和版權管理機際。
數據安全合規	確保合作方遵守隱私,防範數據洩露。
利益分配機制	制定公平合理的收益分成，保障各方利益。
突發事件應對	制定緊急預案,應對技術故障、合作糾紛等突發情況。

最佳實踐：構建多方共贏

1

明確目標

理解核心需求,制定明確的合作目標和預期效果。

2

建立機制

建立規範的信息共享、決策機制。

3

培養信任

注重溝通協調,增進各方的信任和理解。

4

持續優化

定期評估績效,及時調整策略,追求持續創新。

合作模式：靈活多元

聯合開發

多方共同投入資源,共同研發新技術和產品。

技術轉讓

一方將技術授權給他方,獲取專利費。

聯盟

建立長期穩定的合作關係,共同擴張市場。

展望未來：攜手共創成功

追求共融

加強行業內外的溝通。

擁抱變革

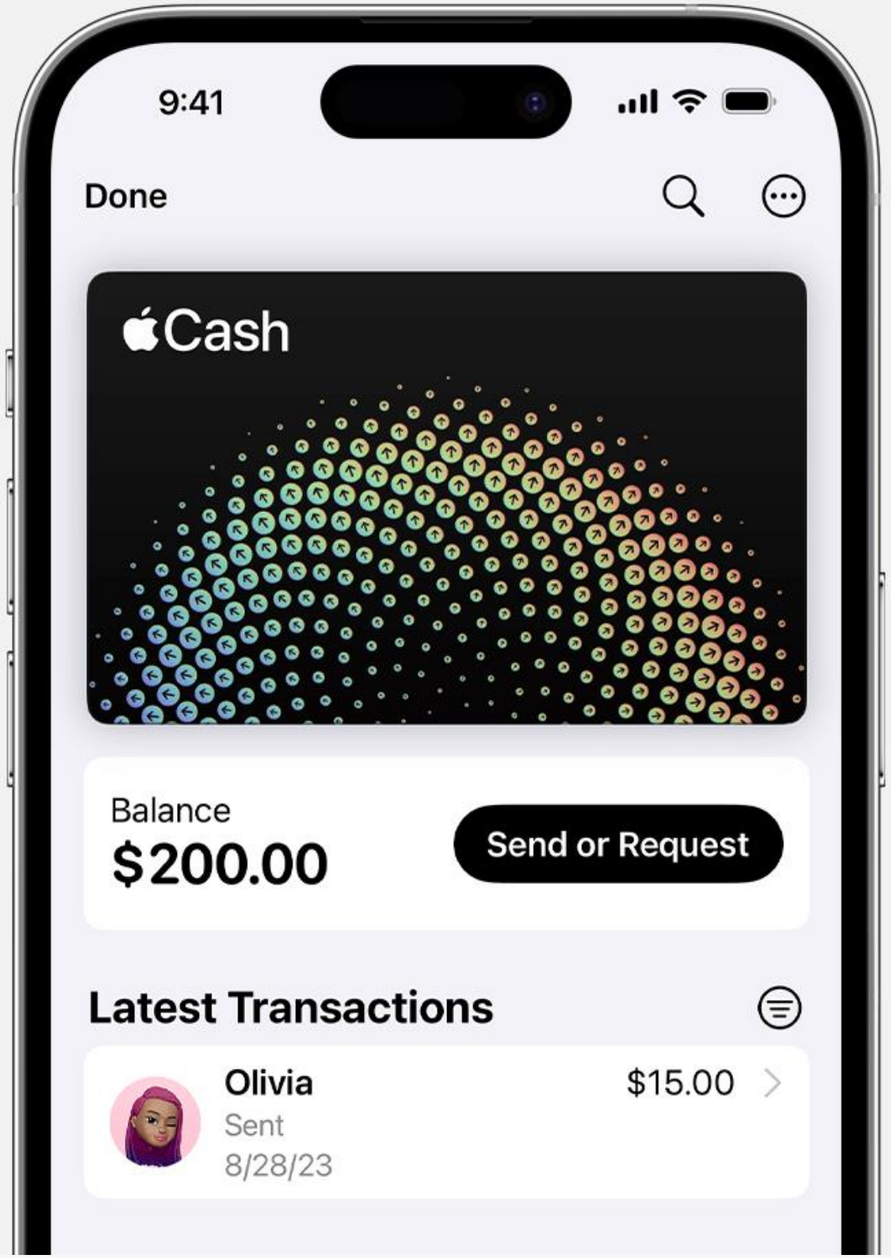
緊跟現時技術發展趨勢,發掘更新智能。

注重用戶

了解用戶需求,提供更加貼心的驗。

規範治理

促進政府、企業與公眾的良性互動,推動健康發展。



移動支付的法規與教育

移動支付作為一種新興的支付方式,其發展和應用受到一系列法規和行業規範的影響。同時,如何提高普通用戶的安全意識也是一個重要的關鍵。

鍾楚真
黃舜朗
林翼亮
李銘軒

法律與行業規範

現有法規

包括《支付服務管理條例》、《非銀行支付機構管理辦法》等,規範了移動支付服務的運營、信息安全方面。

行業標準

業界制定了一系列技術標準和安全準則,如《移動支付業務安全技術規範》,以提高移動支付的安全性。

合規要求

移動支付機構必須嚴格遵守相關法規和行業標準,以確保交易安全和個人信息保護。

法規影響與完善建議

1

保護消費者權益

現行法規有助於維護消費者的合法權益,如限制收費標準、規範退款流程等。

2

提高行業標準

通過制定更嚴格的安全技術規範,提升移動支付的整體安全水平。

3

促進健康發展

適當的法規能為移動支付行業的創新發展創造有利條件。

提升用戶安全意識

1

安全知識普及

通過媒體、學校等渠道,向廣大用戶宣傳移動支付的風險和防範措施。

2

個人信息保護

教育用戶如何保護個人隱私和賬號安全,避免遭受詐騙和盜用。

3

安全操作指引

提供安全使用移動支付的操作說明,幫助用戶養成良好的使用習慣。

4

安全事件報告

建立舉報機制,鼓勵用戶主動上報可疑情況,以便及時處理。

教育與培訓措施

移動支付應用培訓

為用戶提供移動支付應用操作、安全使用等方面的實操培訓。

信息安全教育

加強對用戶的信息安全意識教育,提高個人隱私保護意識。

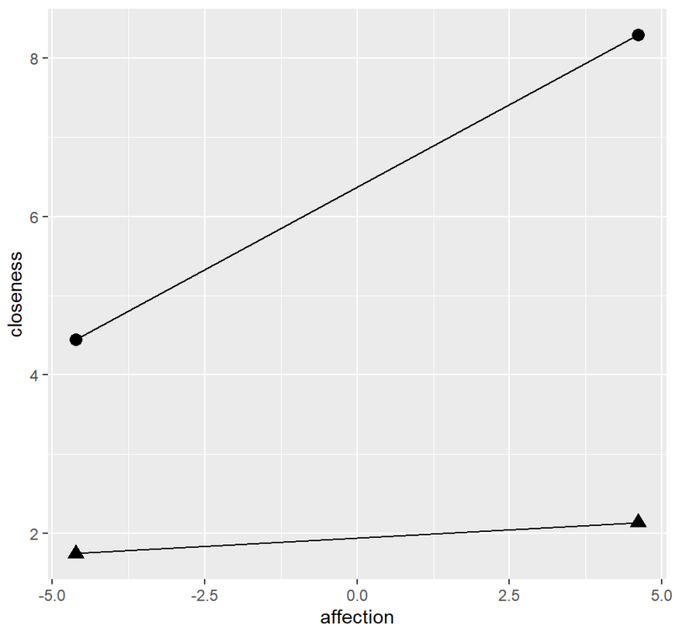
反詐騙培訓

教育用戶識別和防範各種詐騙手段,避免成為受害者。

社區推廣活動

在社區宣傳，讓大眾可了解移動支付的安全問題。

教育培訓效果分析



互動性

採用線上答疑等方式,增強用戶的參與度和學習效果。

持續性

定期更新培訓內容,持續關注移動支付領域的安全動態。

針對性

根據不同群體的特點,設計差異化的教育培訓內容和模式。

未來網絡安全挑戰

支付數據安全

確保大量支付交易數據是否受到安全管理。

新型詐騙手段

隨著技術進步,不斷出現創新的詐騙方式需要防範。

系統漏洞監測

持續識別和修補移動支付系統中的安全漏洞。

防禦策略展望

數據加密保護

採用先進的加密算法和密鑰管理技術,確保數據安全性。

智能監測

利用大數據分析和人工智能技術,實現精準的風險預警和管控。

多層次防護

在移動設備、通信網路、支付系統等環節建立立體的安全防護。

發展趨勢與應用前景

無接觸支付

移動支付將進一步整合各類支付工具,實現快捷、安全的無接觸消費。

生物認證

生物特徵識別技術將廣泛應用於移動支付,提升交易的安全性。

未來發展方向

技術創新

- 生物認證
- 區塊鏈技術
- 5G網絡應用

安全防護

- 多重身份驗證
- 智能風控監測
- 加強數據加密

用戶體驗

- 無縫整合服務
- 個性化定制 - -
-場景擴展

完