香港一卡通手機銀行使用安全提示

1. 請通過招商銀行香港分行官方網站 hk.cmbchina.com 下載，或通過其他招商銀行授權的第三方應用平臺搜尋“香港一卡通”並下載最新的 Android 或 IOS 客戶端。如發現任何可疑的下載程序，切勿嘗試登入及停止操作。

2. 謹防下載假冒手機應用程序，避免被植入釣魚/木馬程序盜取登入數據。如有發現假冒手機應用程序，請及時與本行職員聯繫。

3. 不要複製和安裝不確定來源的手機銀行客戶端軟件。如發現任何不正常運行情況，例如出現異常版面或登入緩慢，請即停止操作。

4. 本行手機銀行採用了嚴密的加密技術，通過一網通賬戶的名稱及密碼或其他驗證要素保障客戶登入安全。我們同時採用嚴格和複雜的風險管理策略，防止異常操作帶來的風險，一旦發現可疑信息，手機銀行將會採取更加嚴格的方式驗證登入和交易。如客戶使用服務時靜止了一段指定時間，登入將被自動終止，防止任何未經授權的交易。

5. 避免使用公眾地方或欠缺密碼保護的無線網絡(即 Wi-Fi)登入手機銀行，建議使用已加密及可靠的網絡連接互聯網以登入手機銀行。

6. 關閉無需使用的無線網絡功能(如 Wi-Fi、藍牙、NFC)。如需使用 Wi-Fi，應選用加密的網絡，並關閉 Wi-Fi 自動聯機設定。

7. 手機應設立自動上鎖和啟用密碼鎖功能，防止他人未經許可使用您的手機，及定期更改手機密碼。

8. 避免於人員擁擠或人流量大的地方登入手機銀行，並留意手機輸入密碼時，有關密碼可能以明碼的方式放大，間接讓第三者窺視登入數據。

9. 為確保您的網上交易安全穩妥，使用手機銀行時，本行會檢查客戶手機操作系統的安全情況，使用破解版本的操作系統或不符合基本保安要求的手機將無法使用本行手機銀行 App，請注意相關提示信息。

10. 每次使用手機銀行時，您可以先核對上一次登入的紀錄；您也應定期檢查賬戶結餘及核對交易紀錄。如發現可疑情況，請及時與本行聯絡。

11. 請牢記密碼，切勿於手機或其他電子設備中儲存您的一網通用戶名稱及密碼。避免使用您容易被他人知悉的信息作為登入密碼，並避免使用於其他網站登記或其他服務的密碼作為登入密碼。切勿讓第三者使用您的手機銀行或密碼。請定期修改手機銀行登入密碼。

12. 如遺失或外洩密碼或遺失手機，或懷疑密碼/手機遭盜用，或發現賬戶有未經授權的交易，請及時與本行聯絡。

13. 當您成功登記【指紋登錄】或【面容 ID 登錄】服務後，任何儲存於您的手機的指紋或面容均能使用【指紋登錄】或【面容 ID 登錄】服務。您必須確保只有您的指紋或面容儲存於您的手機，並確保手機上用作儲存指紋或面容的數據保密。基於安全理由，切勿於您的手機上登記他人的指紋或使用已被破解的手機。

14. 您可以通過登入手機銀行，選擇【設置 > 安全設置 > 指紋登錄/面容 ID 登錄】取消使用【指紋登錄】或【面容 ID 登錄】服務。請您注意於取消服務後，您的指紋和面容數據仍儲存於您的手機上，您可考慮因應情況自行決定刪除有關數據。

15. 如您手機的指紋記錄或面容 ID 曾經變更，您的【指紋登錄】或【面容 ID 登錄】服務可能會被暫停使用，您需要重新登記或啟用【指紋登錄】或【面容 ID 登錄】服務。

16. 安裝病毒防護軟件及個人防火牆來保護您的手機，並定期更新病毒防護軟件。請參考香港計算機保安事故協調中心網頁：https://www.hkcert.org/mobile-security-tools，選擇合適的應用程序。

17. 定期查看本行網頁以獲取有關手機銀行服務有關使用安全的最新信息。

溫馨提示：

1. **本《安全提示》適用於招商銀行香港分行（“本行”）提供的香港分行香港一卡通手機銀行（“手機銀行”）。**
2. **本《安全提示》內容僅供參考，不構成買賣任何服務或產品的要約或要約邀請（有關服務和產品信息請以相關服務及產品條款為准），亦不構成本行的投資意見或建議。**
3. **本《安全提示》的部份內容、數據、觀點和說明，可能引用或涉及來自第三方提供的數據。本行無法保證該等數據來源的完整性和準確性。**
4. **本《安全提示》僅為方便使用者或客戶參閱而設，但不具有約束力，不構成本行對任何特定使用者或客戶的任何具體建議，不對手機銀行任何服務、設施、產品、屬性等作出明示或默示的陳述或保證，也不構成對《香港一卡通手機銀行服務條款及細則》或其他任何手機銀行服務的規管條款的修訂或補充。**
5. **本行將盡合理努力及時更新本《安全提示》，但客戶須知本行將不時更新和修改操作規定、保安程序或其他設置要求而未必作另行通知，閣下可或通過本行網站 hk.cmbchina.com 個人業務部分或其他部分查閱。**