

快速參考指南 強化資訊安全功能

Citi Mobile® 應用程式



啟用強化資訊安全功能



- 1 開啟 Citi Mobile® 應用程式，
點選 [使用現有帳戶登錄]



- 2 輸入您的使用者代碼
和密碼以登入



- 3 閱讀免責聲明，然後點選 [繼續]
以升級 Citi Mobile® 應用程式上的
強化資訊安全



啟用強化資訊安全功能



4

請輸入 6 位數的簡訊 OTP，
並點選 [繼續]



5

強化資訊安全確認畫面。
請注意，一旦啟用強化資訊安全功能，即適用
12 小時的冷卻期間，以限制某些高風險交易。



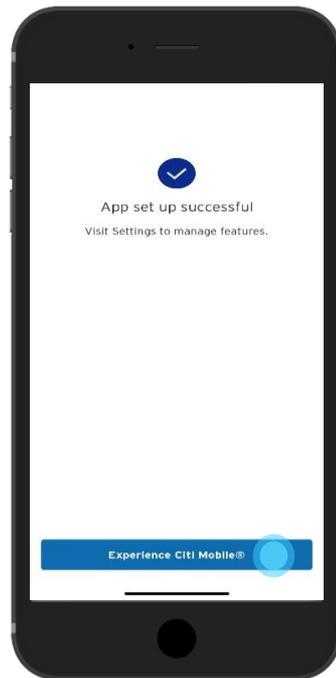
啟用強化資訊安全功能



- 6 若要繼續使用強化資訊安全功能，必須透過 Touch/Face ID® 設定裝置生物辨識驗證，請點選 [開始] 以確認



- 7 成功設定確認畫面



啟用強化資訊安全功能



8

如果您在 12 小時冷卻期間嘗試進行高風險交易，會顯示 [無法繼續] 訊息如下



您的角色與責任

為您的使用者代碼和密碼保密

您不得揭露您的使用者代碼和密碼，並且應確保在輸入使用者代碼、密碼或任何機密資訊時，沒有他人注視。請記住您的使用者代碼和密碼，不要記錄在任何地方。在任何情況下，您都不應向任何人揭露您的使用者代碼和密碼，即使對方聲稱自己是花旗銀行的員工。

請勿透過無法信任的共享電腦或裝置使用網路銀行，例如網咖的電腦。這些裝置可能安裝了某些能夠未經核准就取得個人資訊的軟體。

透過線上資訊安全裝置、Citi Mobile® Token 或透過簡訊產生的一次性密碼 (OTP) 也不應與任何人共享。

行動裝置惡意軟體

以 Android 智慧型手機為目標的行動裝置惡意軟體新變種，持續在亞太地區出現。這些惡意應用程式通常以行動裝置銀行應用程式為目標，並可能試圖竊取客戶認證資訊及執行詐騙交易。

在某些情況下，行動裝置惡意軟體會嘗試透過攔截簡訊 (SMS)，或在行動裝置銀行應用程式內產生虛假對話來欺騙用戶，從而繞過一次性密碼 (OTP) 提供的額外安全層。

花旗建議客戶對惡意軟體威脅保持警惕，並審查我們的線上資訊安全提示。具體來說，花旗建議所有行動裝置用戶考慮：

- 僅安裝來自信任及官方來源的應用程式
- 安裝知名的行動裝置防毒應用程式
- 保持使用行動裝置軟體最新版本
- 知悉已啟用 root 權限或已「越獄」的裝置會面臨較高風險
- 不遵循未知或可疑來源提供的任何連結或指示。

如果發現您的網路銀行作業出現異常行為，應立即終止網路銀行作業，並透過 +65 6224 5757 聯繫 24 小時 CitiPhone Banking。

謹防線上威脅

現今的線上威脅十分猖獗，會誘騙您交出機密資訊。因此，務必了解其機制並採取預防措施來保護自己。

身為網路銀行用戶，您需要扮演的角色，以確保您在使用網路銀行時受到保障。您可以採取下列幾種方法來保護自己：

請務必直接在網頁瀏覽器中，輸入花旗銀行國際個人銀行的網站網址 <http://www.ipb.citibank.com.sg>，確保您是在合法的花旗銀行國際個人銀行網站上輸入用戶代號和密碼以及其他機密資訊。

為了確保您造訪的是安全網站，請檢查瀏覽器網址欄位中的網址開頭，應為「<https://>」而不是「<http://>」。安全網站也會在瀏覽器頂部的狀態列上顯示掛鎖圖示。點選兩次即可檢視頒發給花旗銀行的安全認證。

- 欲驗證網站的真實性，請檢查以下詳細資料：
- 認證頒發給 <http://www.ipb.citibank.com.sg>
- 該認證由 Verisign 頒發。
- 該認證有有效日期。

請在每次作業後清除瀏覽器的快取和歷史記錄，勿在瀏覽器上保存您的網路銀行登入詳細資料。點選此處以了解清除瀏覽器快取的步驟。完成網路銀行作業後，請務必記得登出。

每當您變更詳細聯絡資料時，請務必更新銀行，以便我們在發現任何異常交易時能夠及時聯絡您。

確保您的電腦安裝了最新的防毒軟體，因為這能協助防範新型病毒。電腦的作業系統和瀏覽器軟體應使用最新的安全修補程式進行更新。這些都能協助您的電腦防範未經授權的存取。

您的角色與責任

為您的使用者代碼和密碼保密

您不得揭露您的使用者代碼和密碼，並且應確保在輸入使用者代碼、密碼或任何機密資訊時，沒有他人注視。請記住您的使用者代碼和密碼，不要記錄在任何地方。在任何情況下，您都不應向任何人揭露您的使用者代碼和密碼，即使對方聲稱自己是花旗銀行的員工。

請勿透過無法信任的共享電腦或裝置使用網路銀行，例如網咖的電腦。這些裝置可能安裝了某些能夠未經核准就取得個人資訊的軟體。

透過線上資訊安全裝置、Citi Mobile® Token 或透過簡訊產生的一次性密碼 (OTP) 也不應與任何人共享。

行動裝置惡意軟體

以 Android 智慧型手機為目標的行動裝置惡意軟體新變種，持續在亞太地區出現。這些惡意應用程式通常以行動裝置銀行應用程式為目標，並可能試圖竊取客戶認證資訊及執行詐騙交易。

在某些情況下，行動裝置惡意軟體會嘗試透過攔截簡訊 (SMS)，或在行動裝置銀行應用程式內產生虛假對話來欺騙用戶，從而繞過一次性密碼 (OTP) 提供的額外安全層。

花旗建議客戶對惡意軟體威脅保持警惕，並審查我們的線上資訊安全提示。具體來說，花旗建議所有行動裝置用戶考慮：

- 僅安裝來自信任及官方來源的應用程式
- 安裝知名的行動裝置防毒應用程式
- 保持使用行動裝置軟體最新版本
- 知悉已啟用 root 權限或已「越獄」的裝置會面臨較高風險
- 不遵循未知或可疑來源提供的任何連結或指示。

如果發現您的網路銀行作業出現異常行為，應立即終止網路銀行作業，並透過 +65 6224 5757 聯繫 24 小時 CitiPhone Banking。

免責聲明

一般免責聲明

本文件的內容僅供一般資訊和說明之用，並非財務、投資或任何其他類型的建議。若於任何司法管轄區散佈或要約行為未經授權，或對任何人散佈此等文件或進行任何要約或招攬係屬違法，本文件不構成於該等司法管轄區散佈任何資訊，或進行任何要約或招攬。某些產品和服務在部分司法管轄區可能無法提供。您應向專業顧問諮詢您是否需要政府或其他方面的同意，或需要遵守任何程序，以使用或購買本網站提及之產品和服務。實際產品和服務可能會因功能改進而有所不同。花旗銀行新加坡有限公司不對客戶或任何其他人士因存取或使用本文件、或使用本文件中包含的任何資訊，而直接或間接遭受或產生之任何性質的損失或損害（包括衍生性損失或損害）負責。

花旗銀行的完整免責聲明、條款與條件，適用於個別的產品及銀行服務。如需更多資訊，請造訪 www.ipb.citibank.com.sg。

立即登入 在 Citibank Online 和 Citi Mobile[®] 上探索這些功能

線上提供的主要功能



服務

目前餘額、最久 7 年的對帳單以及 2 年的通知書



投資

外匯、定存、債券、經紀、特惠帳戶、投資基金



銀行業務

電匯轉帳、花旗全球速匯



Citibank Online
www.ipb.citibank.com.sg

Citi Mobile[®] 應用程式



新加坡花旗銀行國際個人銀行



www.ipb.citibank.com.sg



8 Marina View
#21-00 Asia Square Tower 1
Singapore 018960



銀行營業時間
星期一至星期五：上午 9:30 – 下午 6:00

