2023 年 11 月 30 日 | 重要消息

暫停 Android 裝置的螢幕截圖及錄影功能
防範惡意軟件攻擊 保障客戶安全

Livi Bank Limited（「livi」或「本行」）提醒客戶及公眾人士慎防惡意軟件騙案。鑑於近日市面上有騙徒誘騙用戶下載帶有惡意軟件的手機應用程式，獲取客戶登入銀行的資料及密碼，本行已暫停個人及企業客戶以 Android 裝置於 livi 手機應用程式的螢幕截圖及錄影功能，以保障客戶安全。

個人及企業客戶如須留存各項交易的紀錄，可登入 livi 手機應用程式，點選界面下方的「交易紀錄」，客戶亦可點擊各項紀錄查看最近一年內的交易詳情。如有需要儲存記錄至流動裝置，可於交易詳情頁面按左下角的「下載交易通知書」，畫面出現「成功儲存」提示，即表示交易之圖像記錄已存至裝置的相簿或照片庫中。

本行呼籲客戶及公眾人士切勿下載任何未經認證的手機應用程式，或點擊經短訊、電郵或網站等渠道傳送的可疑連結，提供任何個人資料或進行任何交易。如有懷疑或未能確定網站的真偽，可致電香港警務處反詐騙協調中心「防騙易 18222」熱線尋求協助。

任何人士如曾向任何未獲本行授權的網站或手機應用程式提供其個人資料或處理任何交易，請即向香港警方求助，及致電 livi 客戶服務熱線（852）2929 2998 或電郵至 livicare@livibank.com 與本行聯絡。

本行同時提醒客戶須提高警覺，慎防受騙：

- 切勿點擊可疑短訊、電郵、附件、網頁，社交平台頁面/發文內或來歷不明的超連結。如有懷疑，請即停止操作，切勿輸入任何資料，關閉視窗，並刪除相關手機應用程式；
- 只從官方應用程式商店下載及安裝由可信任及已認證開發商提供的手機應用程式；
- 在安裝前及每次被提示時應先仔細評估相關手機應用程式的權限需求，如果發現可疑的權限需求，切勿安裝相關手機應用程式或立即將其刪除；
- 切勿用 Jailbreak（越獄）或 Root 等手法破解或改裝流動裝置；
- 定期經可信渠道安裝應用程式更新以及操作系統和瀏覽器的更新和修補程式，切勿從任何不可靠來源下載程式或軟件。

本行不時於本行網站更新欺詐資訊提示，詳情請瀏覽 https://www.livibank.com/zh_HK/important-notices.html。有關電子銀行服務的保安提示，請瀏覽 https://www.livibank.com/zh_HK/security-tips.html。

Livi Bank Limited
28/F Oxford House, Taikoo Place
Quarry Bay, Hong Kong