BEA東亞銀行

東亞銀行有限公司澳門分行
（「東亞銀行澳門分行」）
東亞澳門手機銀行保安提示

問題1：我可以如何識別由銀行發出之短訊？

為協助市民識別短訊發送人的身分，東亞銀行有限公司(「東亞銀行」)已參與及成為由香港通訊事務管理局辦公室推出的「短訊發送人登記制」之「已獲認證的發送人」。

由2024年1月28日起，所有東亞銀行於香港發送之短訊會使用以「#」號為開頭，表明短訊是由「已獲認證的發送人」所發出。東亞銀行亦會為持有香港手機號碼的澳門分行客戶發送短訊，而相關的「已登記的短訊發送人名稱」將包括：

- #BEAMO
- #BEA_MO
- #BEA-MO

「短訊發送人登記制」並不適用於：

(1) 可供接收者以發送人號碼直接回覆的短訊；或

(2) 使用非香港營辦商提供之一卡多號/一卡雙號流動服務的香港用戶。

有關「短訊發送人登記制」的詳情，請瀏覽香港通訊事務管理局辦公室網站(www.ofca.gov.hk/ssrs)。

東亞銀行提醒您在任何情況下，當收到陌生人發送的短訊時，都應提高警惕。絕不要向身分未經核實的短訊發送人披露個人、銀行戶口或信用卡資料、轉賬金錢或開啓短訊內的超連結，以免蒙受損失。

問題2：為什麼我的流動裝置會有潛在的安全風險？

當使用東亞澳門手機銀行時，如我們偵測到你的流動裝置安裝了列入黑名單或從非官方渠道下載的應用程式並授予過多的權限，螢幕將會顯示安全警告提示。我們會限制該部流動裝置使用東亞澳門手機銀行。

BEA東亞銀行

問題3：我如何恢復使用該流動裝置登入東亞澳門手機銀行？

你可以選擇以下其中一個方法恢復使用該部流動裝置登入東亞澳門手機銀行。

方法1 (建議做法)

根據東亞澳門手機銀行顯示的安全警告提示，刪除被列為有潛在風險的應用程式；或

方法2

透過裝置設定 > 協助工具 / 無障礙設定，關閉被列為有潛在風險應用程式的無障礙設定，以避免他人透過此設定存取你的個人資料，令重要資料外洩。

問題4：我如何關閉被列為有潛在風險應用程式的無障礙設定？

就不同的流動裝置製造商及作業系統，更改協助工具 / 無障礙設定的方法可能會有所不同。

一般而言，客戶可於流動裝置內的「設定」>「輔助功能」/「無障礙功能」> 在「已下載的應用程式」中選擇有潛在風險的應用程式 > 關閉應用程式的無障礙設定。

問題5：我如何在此流動裝置上重新使用東亞澳門手機銀行？

你可以：

- 使用東亞銀行建議的操作系統及透過官方應用商店(如: Google Play 或 App Store)下載東亞澳門手機銀行
- 檢查流動裝置之安全性及
- 檢查此流動裝置中的應用程式 及
- 移除可疑的應用程式及 / 或
- 禁止安裝來源不明的應用程式並維持適當設定及 / 或
- 停止流動裝置上網站、應用程式及其他軟件/程式不尋常或不必要的請求，及 / 或
- 確保裝置上的作業系統及應用程式已裝有最新的安全更新或考慮使用最新的保安軟件 / 程式不時掃瞄你的裝置以加強保安。

問題6：我如何更有效地確保裝置安全？

- 為確保交易安全，請透過官方應用商店 (如: Google Play 或 App Store)下載流動應用程式。
- 確保裝置上的作業系統及應用程式已裝有最新的安全更新，切勿在「超級用戶權限破解」的流動裝置使用東亞澳門手機銀行。安裝防毒軟件並更新至最新版本及定期掃瞄你的流動裝置。

BEA東亞銀行

問題7：有甚麼保安提示以確保安全使用東亞澳門手機銀行？

保護你的賬戶及密碼

1. 切勿以身份證號碼、電話號碼、出生日期、駕駛執照號碼或任何常用之數位組合 (如987654或123456) 作為你的密碼，及不應使用同一數字或英文字母多於兩次。
2. 請牢記你的密碼，切勿用筆記下。
3. 請經常透過東亞澳門手機銀行更改你的密碼。避免重複使用個人賬戶和／或社交媒體賬戶中的密碼。
4. 在任何時候，必須將你的使用者號碼及密碼保密。在任何情況下，請確保你（及有關連的任何被授權人士）不向任何其他人士或軟件（包括任何聯名賬戶持有人或任何財務管理軟件／程式）披露或分享，及將此等資料以電子郵件、或任何即時通訊軟件／程式傳送。你亦不應將相同的密碼用於其他服務（如接駁互聯網或登入其他網站）。此外，設定與你其他個人賬戶明顯不同的登入資料，用戶名稱和／或 密碼，尤其是社交媒體賬戶。
5. 在任何情況下，東亞銀行有限公司澳門分行絕對不會使用電子郵件、手機短訊、或任何即時通訊軟件／程式、電話或任何其他方式要求你提供個人資料，如密碼、一次性密碼、身份證號碼、出生日期、賬戶／信用卡號碼、信用卡到期日、電話號碼、東亞澳門網上銀行賬戶號碼／使用者姓名或手機銀行使用者號碼等資料。在任何情況下，不可將此等資料告知任何人，包括自稱為東亞銀行澳門分行代表或僱員的人士。
6. 請刪除所有在使用流動理財服務後收到的手機短訊／推送訊息。
7. 當發覺或懷疑你的密碼未經授權而被他人使用時，必須立即通知東亞銀行澳門分行，並即時以書面確認。
8. 當進行銀行交易時，須先留意四周環境，切勿讓第三者得知你的密碼。當在任何裝置（如個人電腦、流動裝置）或自助／公眾終端機輸入密碼時，請遮掩按鍵。
9. 切勿在使用東亞澳門手機銀行時離開你的裝置，亦不要讓任何人使用你的手機銀行。
10. 切勿透過公眾電腦或公共無線網絡登入手機銀行。當使用Wi-Fi登入手機銀行時應選用加密的網絡，並移除不必要的Wi-Fi連線設定。如無須使用無線網絡功能（如Wi-Fi、藍芽、近距離無線通訊（ NFC））或支付應用程式，請謹記關閉此功能。
11. 如懷疑已被偽造網站、偽造電子郵件，或透過公共無線網絡、公用電腦、第三者裝置或任何其他方式欺騙（例如：輸入正確密碼後不能登入有關服務網站，無論有沒有顯現任何警告訊息），請立即更改密碼。
12. 切勿啟動流動網絡供應商提供之短訊轉線功能。因你的電腦如被惡意程式入侵，騙徒可在你透過電腦使用本行之服務時盜取你的個人資料，如密碼、賬戶及手機號碼等。在此情況下，騙徒會啟用你的短訊轉線功能，將東亞銀行澳門分行發送給你的短訊交易密碼轉至其流動裝置。藉此，騙徒能沿用你的個人資料及該短訊交易密碼從你的賬戶提取款項。

BEA東亞銀行

提防網上安全威脅

1. 切勿經任何電子郵件、手機短訊、即時通訊訊息、二維碼、搜索引擎或任何不可靠來源內的網址或超連結登入手機銀行。切勿使用東亞澳門手機銀行以外的應用程式、程式或軟件登入手機銀行。
   客戶應直接於瀏覽器的網址列內輸入www.hkbea.com.mo或透過東亞澳門手機銀行以瀏覽東亞銀行澳門分行網頁，或將真確的網址設為書籤以便以後到訪。
2. 請注意東亞銀行澳門分行或其代理／業務合作夥伴不會向你發送帶有超連結或二維碼的電子郵件，其中包含指向交易網站或流動理財應用程式的超連結。
3. 當收發電子郵件、開啟電子郵件附件、進入及告知個人／財政資料予不知名網站及下載網站內的檔案或程式時，請慎防駭客、病毒、間諜軟件及任何其他惡意程式入侵。切勿瀏覽可疑網站及開啟可疑電郵，包括但不限於加密文件，壓縮文件（zip），或透過WhatsApp、Line、微信及其他電子媒體所接收訊息內的超連結及附件。
4. 切勿使用來歷不明的應用程式、程式或軟件。

保護你的裝置

1. 使用東亞銀行澳門分行建議的操作系統、東亞澳門手機銀行及瀏覽器版本登入手機銀行。切勿用 Jailbreak（越獄）或Root機等手法改裝你的流動裝置。
2. 切勿於你的裝置上安裝或運行來自第三方的應用程式。建議在你的裝置上設定禁止安裝來源不明的應用程式並維持適當設定。
3. 細閱網站、應用程式及其他軟件／程式的安裝或許可請求，警惕任何不尋常或不必要的請求。
4. 確保你裝置上的作業系統及應用程式已裝有最新的安全更新。
5. 考慮使用最新的保安軟件／程式不時掃瞄你的裝置以加強保安。
6. 不時檢查你裝置中各應用程式對儲存空間的用量、耗電量及流動數據用量，以偵察任何可疑的應用程式。必要時，移除任何可疑應用程式。
7. 切勿與他人共用你的裝置或使用他人的裝置登入東亞澳門手機銀行或東亞澳門網上銀行。為你的裝置設定難以猜破的鎖機密碼及啟動自動上鎖　功能。
8. 如你的裝置能夠使用生物認證（如手指紋或面容辨識），切勿讓任何人在你的裝置上登記其生物信息。
9. 如你有多胞胎或面容相像的兄弟姊妹，或正處於面部特徵可能快速發展的青春期，　請不要使用面部辨識作認證。
10. 切勿停用任何有助提升生物認證安全性的功能，例如面部辨識功能內可感知客戶注視流動裝置的功能（如確保已開啟「使用Face ID需要注視螢幕」）。