

安全使用網上銀行的八條溫馨小提示

1 定期監控帳戶

確保所有的交易都由本人親自授權。如果發現任何可疑的欺詐活動，請立即向銀行報告

2 警惕奇怪的電子郵件！

如果您收到聲稱是銀行（或其他公司）發出的電子郵件，並要求您提供帳戶詳細資訊或密碼，請千萬不要回復。銀行不會通過電子郵件索取個人使用者的帳戶資訊

3 不要點擊電子郵件中的連結

請儘量手動登錄網上銀行，以確保您所進入網站的安全性

4 定期更改銀行密碼

不要在多個網站使用相同的密碼，並確保選擇一個包含大小寫字母、數位和特殊字元的高強度密碼。不要使用包含個人姓名、首字母或出生日期的任何詞語或短語

5 啟用雙重身份驗證

多數金融機構為帳戶持有人提供額外的安全保護——雙重身份驗證，即要求用戶在登錄帳戶之前進行額外驗證

6 禁用自動登錄

禁止網路瀏覽器保存網上銀行的登錄用戶名和密碼

7 儘量使用銀行的官方APP

確保從可靠來源（如Apple Store或Google Play Store）下載APP

8 不確定某個事件是否合法？

對網銀技術存在疑問？請致電工作人員，他們將樂意幫助您！

資訊由以下機構合作提供：



加強網路安全的八條溫馨小提示

1 電子郵件欺詐

如果郵件內容好得令人難以置信，比如說告訴您“中大獎了”或“外國王子聯繫您”，那很可能就是欺詐，千萬不要相信！

2 欺詐性支付

如果您收到支票、本票、匯票或電子資金轉帳後，要求您退還部分金額，請謹慎處理，很可能是欺詐

3 主動提供的優惠

若收到“超值驚喜，欲購從速”等資訊，要謹慎對待

4 保持更新

確保設備的作業系統（如Windows、Apple IOS、手機IOS（Apple、Android等））的安全設置更新到最新版本

5 警告和錯誤提示

不要相信彈出警告或錯誤提示的網站

6 小心電子郵件的附件

謹防點擊來自未知來源的電郵附件或免費軟體，否則可能面臨線上欺詐和盜竊的風險

7 線上分享

注意在網上分享的內容。您在社交網站上發佈的個人資訊越多，就越有可能會有人利用這些資訊來訪問您的帳戶、竊取您的身份。您需要通過加強隱私設置來保護個人資訊

8 金融詐騙

注意與災害事件相關的金融詐騙。騙子可能聲稱自己來自合法的慈善組織，在災害事件後騙取人們的信任，而實際上是為了竊取金錢或有價值的個人資訊

更多有關線上安全的資源：

Texas Department of Banking – www.dob.texas.gov

Texas Bankers Association –
www.texasbankers.com/BankingSafely

Better Business Bureau – www.bbb.org/council/for-businesses/cybersecurity/