

信用卡小錦囊

感謝 閣下對華僑銀行(香港)有限公司(“本行”)信用卡的支持。為進一步讓 閣下了解信用卡安全小貼士及信貸資料之安排，請留意以下各點：

網絡釣魚及惡意軟件

- 慎防網絡釣魚。接收到電子郵件或短訊時，檢查發送人之身份，對不明人士或已長期沒有聯絡的朋友的電子郵件或短訊保持警覺，切勿點擊或下載任何可疑的連結或附件或掃描二維碼。
- 提防騙徒假冒銀行或其他公司通知您中獎或有積分換領，要求您提供您的個人資料、信用卡資料及/或一次性密碼的電子郵件或短訊。
- 切勿向任何人透露您的一次性密碼。
- 切勿瀏覽不安全的網站、點擊任何在社交媒體或手機應用程式上的可疑廣告連結或下載任何惡意軟件¹。
- 本行不會發出含有超連結要求您登入網上理財或輸入個人資料的電子郵件或短訊。
- 安裝防毒軟件及定期更新軟件，以辨識病毒檔案及預防電腦被病毒感染。

電話詐騙

- 當收到不明人士、自稱政府官員或自稱電訊公司、公營機構或銀行職員的可疑來電，請先確認對方身份，詢問來電者如何取得您的電話號碼及戶口資料，如來電者拒絕透露便應終止對話。
- 騙徒會以欺詐手法(如訛稱有特別優惠、假冒政府官員、訛稱速遞公司或郵局員工通知您有欠資包裹可取等)，騙取您的個人資料如銀行或信用卡資料以進行交易或轉賬。提高警覺，慎防洩露您的個人資料或信用卡資料給陌生人。

網上交易及網上/流動理財

- 輸入一次性密碼前，先檢查短訊內容，包括商戶名稱、

交易金額、交易貨幣等資料，以確保與將進行之交易內容一致。

- 透過官方渠道或信譽良好的平台進行網上購物，並於進行交易前清楚了解有關退款及退貨的政策及細則。
- 切勿連接任何不安全或沒有加密之網絡系統及於公用電腦或他人的電子設備輸入信用卡號碼、密碼、其他個人資料及登入流動理財服務。
- 切勿在瀏覽器儲存任何信用卡或個人資料，並對以自動填寫功能輸入之資料保持警覺。
- 每次使用網上及流動理財服務後，請照指示登出。

日常注意

- 收到信用卡後立即於背面簽署，並妥善保管信用卡，切勿隨意擺放。
- 切勿向任何人士透露您的信用卡號碼、密碼、驗證碼及其他個人敏感資料，除非您知道這是合法的要求。
- 在緊記密碼後，請將密碼函件銷毀。
- 切勿將密碼寫下或將密碼的任何紀錄與信用卡存放在一起。
- 避免以身份證號碼、電話號碼或出生日期等容易猜測的號碼作密碼。
- 定期更改密碼，切勿與其他平台共用同一密碼。
- 輸入敏感資料前應提高警覺，留意附近是否有可疑人士窺探以防資料外洩。
- 簽賬後或完成自動櫃員機交易後，緊記取回信用卡，並定期檢查以確保沒有遺失。
- 支付前，核對交易金額，並保留賬單副本以便核對。
- 仔細查核信用卡月結單及交易通知，確保沒有未經授權之交易。
- 慎防偽冒本行的來電，本行不會以電話或電郵要求客戶提供敏感個人資料。

保障自己

- 如有懷疑騙案，請盡快通知本行，及聯絡香港警務處反詐騙協調中心「防騙易18222」熱線。
- 如發現有可疑交易，請立即致電我們的客戶服務熱線(852) 2543 2223。
- 作為持卡人，請時刻妥為保管您的信用卡、信用卡賬戶號

碼及私人密碼，因您須對因沒有履行前述責任而導致之一切損失承擔責任。

- 一經發現信用卡、信用卡賬戶號碼或私人密碼遺失、失竊、未獲授權使用、不正當使用及/或外洩，請您立即致電本行的熱線 – 香港(852) 3199 9000或澳門(853) 2838 8144通知本行。在本行**未接獲**您前述的通知之前，作為持卡人，您須對信用卡賬戶之一切結欠**負全責**，不論該等結欠是否因任何未獲授權或不正當使用信用卡、信用卡賬戶號碼或私人密碼所引致。有關持卡人責任詳情，您可於本行網站細閱持卡人協議。
- 想了解更多提防詐騙資訊，可瀏覽香港金融管理局網頁及/或社交頻道瀏覽相關影片了解詳情。
- 如任何個人資料(包括通訊地址及聯絡電話)有所更改，立即通知本行作資料更新。

查閱信貸資料之安排(如適用)

本行或會在未來12個月，就 閣下現行之信貸安排(包括但不限於更改信用額、取消信貸或債務安排計劃之執行)進行審查，並可能會**多於一次**查閱 閣下於信貸資料服務機構內的信貸資料。 閣下亦可直接致電本行客戶服務熱線作有關查詢。

如有任何查詢，歡迎致電本行的客戶服務熱線(852)2543 2223。如本函中英文版之內容有歧義，一概以英文版為準。

華僑銀行(香港)有限公司 謹啟
2023年11月

¹ 惡意軟件是指未經用戶同意下安裝在用戶的電腦或手機上的非法且難以察覺的軟件，從而入侵、破壞電腦系統、盜取用戶個人資料等進行不法行為。

Credit Card Tips

Thank you for your support on OCBC Bank (Hong Kong) Limited ("Bank") Credit Card. To provide more information in relation to credit card security tips and access to credit data arrangement, please refer to the followings:

Phishing and Malicious Software

- Stay alert to phishing. Verify sender's identity when receiving an email or SMS and be vigilant to the email or SMS from an unknown person or a person who has not contacted for a long time. Do not click the hyperlink or download the attachment or scan the QR code which is suspicious.
- Be vigilant to phishing email or SMS from fraudsters impersonating bank or other company, claiming that you have won a prize or you have points for redemption, to request your personal information, credit card numbers and/or One-Time-Password.
- Do not disclose your One-Time-Password to any person.
- Do not visit unsecured website, click the advertising hyperlink on social media platforms or mobile's apps which is suspicious, or download any Malicious Software¹.
- The Bank will never send you email or SMS with embedded hyperlink for logging to internet banking or entering your personal information.
- Install antivirus software and update the application regularly to detect virus and prevent virus infection.

Telephone Deception

- When you receive a suspicious incoming call from unknown person or someone claiming to be a government official or a staff of a telecommunication company, public sector or a bank, please confirm the caller identity and ask the caller how he/she has your phone number and account information. Terminate the call if the caller refuses to answer.
- Scammers will use fraudulent tactics (e.g. claiming to have special offer, pretending to be a government official, pretending to be a staff of courier company or Post Office notifying you of an underpaid parcel, etc.) inducing you to disclose your personal sensitive information such as bank or credit card information to conduct purchase or fund transfer. Stay alert and avoid disclosing your personal information or credit card information to strangers.

Online Payment and Internet/ Mobile Banking

- Check the SMS content, including merchant's name, transaction amount and transaction currency etc., to ensure it is the transaction you are performing before entering a One-Time-Password.
- Always purchase through official sales channels or reputable online

platforms and fully understand the relevant terms and policies in relation to product refund and return before engaging in any transaction.

- Never connect to any unsecured or unencrypted network and do not enter your credit card number, password, other personal information and login internet banking/ mobile banking in public computers or other's electronic devices.
- Never save any credit card or personal information in web browsers and stay alert to the information inputted by auto-fill function.
- Every time you use online or mobile banking services, please make sure you follow the proper log-out procedure.

Daily Attention

- Sign on the card back once you receive it, keep it safe and never leave it unattended.
- Do not disclose your credit card number, password, verification code or other personal sensitive data to anyone unless you know it is a legitimate request.
- Destroy the PIN mailer after memorizing the PIN.
- Do not write down the PIN or keep any record of the PIN with your credit card.
- Avoid using numbers that can be easily guessed such as your ID card number, telephone number or date of birth etc. as password.
- Change your password regularly. Use a separate password which is not used for other platforms.
- Stay alert to people snooping around you when entering sensitive data to avoid data leakage.
- Remember to retrieve your credit card after purchase or completing ATM transaction and check it regularly to ensure it is with you.
- Verify the transaction amount before payment and keep a copy of your sales slip for the purpose of verification.
- Review your credit card monthly statement and transaction notification to ensure there is no unauthorised transaction.
- Stay alert to fraudulent calls purportedly from the Bank. The Bank never asks you to provide sensitive personal information via phone call or email.

Protect Yourself

- If there is any suspicious scams, please inform the Bank immediately and contact the Anti-Deception Coordination Centre (ADCC) of the Hong Kong Police Force through the "Anti-Scam Helpline 18222" hotline.
- If you have discovered any suspicious transaction, please contact our Customer Service Hotline immediately at [852] 2543 2223.
- As a cardholder, please keep the credit card, the credit card account number and the PIN safe at all times under your own control. You are fully responsible for all losses resulting from your failure to do so.

- Please notify the Bank at [852] 3199 9000 (Hong Kong) or [853] 2838 8144 (Macau) immediately upon discovery of the loss, theft, unauthorized use, misuse and/ or disclosure of the credit card, the credit card account number or the PIN. As a cardholder, you are **fully liable** for all amounts that the Bank debit to your credit card account whether due to the unauthorized use or misuse of your credit card, the Card Account Number or the PIN **before the Bank receives the aforesaid notification**. For the details of cardholder's liabilities, please refer to the Cardholder Agreement available at the Bank's website.
- To learn more anti-fraud and prevention tips, please visit Hong Kong Monetary Authority's website and/ or social media to watch the relevant videos.
- Inform the Bank immediately for information update if there is any change in your personal particulars (including correspondence address and contact number)

Access to Credit Data (If applicable)

During the next 12 months, the Bank may access your consumer credit data held by the credit reference agency(ies) **MORE THAN ONE TIME** for the purpose of reviewing your existing consumer credit facilities (including but not limited to credit line adjustment, cancellation of credit or implementation of a scheme of arrangement). You may also check the relevant details by calling our Customer Service Hotline.

For any enquiries, please contact our Customer Service Hotline at [852] 2543 2223. If there is any inconsistency or conflict between the English and Chinese versions of this notice, the English version shall prevail.

OCBC Bank (Hong Kong) Limited
November 2023

¹ Malicious Software means an illegal and imperceptible software installed on user's computer or mobile without user's consent. Thereby, it will be invading and destroying the computer system, stealing the user's personal information, and committing illegal acts.