HSBC Broking Services (Asia) Limited

Online Security Tips for accessing Digital Trading Services

HSBC

OCT 2022

Content

- Accessing Digital Trading Services securely
- Protect your passwords
- How we protect you online
- Important notes

- Avoid accessing your Digital Trading Services (the "Services") account at public computers or public Wi-Fi networks. Use security protection such as Wi-Fi Protected Access (WPA), if possible.
- Only use trusted Wi-Fi networks or service providers to accessing your account of the Services.
- Do not disclose your personal details, e.g. username, password and security code, to anyone.
- If you find any unusual pop-up screen or computer response is unusually slow, please do not input your personal details or any account information and report to customer service hotline.
- Do not use hyperlinks to access the Services unless you are sure that they are from secured sources. Instead, enter the website address directly, such that you can avoid being brought to a fraud site.
  Remember: HSBC Broking will never provide any hyperlink to the logon page by emails or SMS.
- HSBC Broking is not affiliated with any third party aggregator mobile apps and for security reasons customers should not disclose their digital trading services credentials, especially one-time security code to third parties.
- Only use trusted mobile devices to access the mobile trading app, such that your log on credential will not be captured by a fraudulent device.
- Always check the date/time of your last logged on session. This information is available on the welcome page when you logon to the Services.
- Do not let your browser remember your logon details for accessing the Services.
- Always verify that the website you are visiting is genuine. Click the 'padlock' icon at the top of the page near the address bar to ensure that the identity of the website is certified as **https://www.hsbc.com.hk/broking/**.
- Ensure the HSBC Broking mobile trading app (the "app") you are using is genuine. Only download the app from Hong Kong App Store or Google Play Store and verify the developer of the app is "The Hong Kong and Shanghai Banking Corporation Ltd". This ensures that the apps you download are authentically from HSBC Broking.
- Always exit by clicking the 'Logoff' button to ensure that you have ended the session securely.
  Remember: Closing the browser window does not ensure that your session is terminated properly.

- Never share your password to anyone.
- Do not forward your one-time password (OTP) / security token to others.
- Change your password on a regular basis (e.g. every month) and select password combination that are difficult to guess.
- New password should be different from your previous twelve passwords.
- Use different passwords for different websites and channels.
- Memorize your password and do not write it down.
- Don't use the word 'password', numerical sequences (for example "12345"), easily recognised keypad patterns ("14780", "qwerty", etc.) or a single commonplace dictionary word that could be cracked by common hacking programs.
- Avoid sharing your device and account password with others and do not use other people's devices to log on to your private accounts.
- HSBC Broking staff will never ask you to provide passwords, over the phone, nor will we notify you of account irregularities using pre-recorded messages.

- We will send a system generated identification ("Registration UID") and a system generated password ("Registration PIN") to you. You will need this information for your first time registration of the Services. To learn more about Registration UID and Registration PIN, please **click here**.
- When you logon to the Services, your account is protected by a combination of 1) a unique username; 2) a password; and 3) a second password or a one-time 6-digit password generated by your security device. To learn more about security device, please **click here**.
- If you use the "dual password" mode to log on to the Services and wish to perform any trade-related activity or review your personal information, you will be prompted to input a one-time 6-digit password ("security code") either received via short message service or generated by a security device. This aims to strengthen the identity authentication measures. Remember to update your mobile number registered with us as soon as possible if the number has changed. To learn more about security code, please **click here**.
- You will receive email notifications when you performed the following activities successfully: 1) logon to the Services; or 2) change your passwords through the Services; or 3) any trade instruction placed by you through the Services. If the activity mentioned in the email notification is not performed by you, please contact our customer service hotline for assistance immediately. Remember to update your email address registered with us as soon as possible if the email address has changed.
- As a security measure, you will be automatically logged out of the Services if you do not do anything on a page for a certain period of time. You should always log out from the services when you have finished.
- To protect you and our systems, some of the oldest web browser versions will no longer be able to access to the Services. Generally, the latest versions of a browser (such as Microsoft Internet Explorer, Google Chrome and Apple Safari) have the most up-to-date security features. If you are not using recent browser versions, please upgrade your browser to the latest version. You can search online for advice on how to do this.
- When using our App, please update to the latest version to ensure a safer and smoother user experience.

- Everyone should be wary of online phishing scams. Phishing is an attempt by criminals to 'fish' for personal information such as security credentials, or to convince you to click on or open malicious files/links.
- You should install firewalls and anti-virus software to counter viruses and spyware. Most computers come with personal firewalls – known as software firewalls – pre-installed. For additional security, you can download an additional stand-alone firewall, known as a hardware firewall. For anti-virus and anti-spyware software, there are many kinds available on the market. Always use a reputable brand and be mindful of fake products.
- Always check SMS, email notification, statement and email message issued by HSBC Broking.
- Stay vigilant to any unfamiliar SMS / email / call / website which have a different look and feel, or content from a regular HSBC Broking SMS / email / call / website. Pay attention to the domain of email and website, do not reply or click on any links, or open any attachments if you suspect any phishing activities
- Ensure your mobile number and email address registered with us are valid and updated.
- If you suspect any unusual activities in your account or receive any suspicious SMS/email/phone call asking you for your logon or personal details, please contact HSBC Broking's customer service hotline at (852) 3989 8181. The hotline service hours are from 8.30am - 5.30pm Mondays - Fridays (except public holidays).
- For more information about online security, please go to "Online Security" at the bottom of the homepage of HSBC Broking's public website: **www.hsbc.com.hk/broking**

滙豐金融服務(亞洲)有限公司

網上交易服務保安提示

HSBC
滙豐

2022年10月

目錄

- 避免使用公用的電腦或公用的Wi-Fi無線網絡登入網上交易服務（「服務」）。盡可能採用保安措施，例如Wi-Fi Protected Access（WPA；一種保護無線電腦網絡安全的系統）。
- 只使用可信賴的Wi-Fi無線網絡或服務供應商登入服務。
- 切勿將您的個人資料（例如用戶名稱、密碼和保安編碼等）給予任何人。
- 如果您發現任何不尋常的彈出式視窗或電腦反應異常緩慢，請勿輸入您的個人資料或戶口資料，並致電客戶服務熱線通知我們。
- 切勿使用超連結連接到服務網站，除非您確定該超連結是安全及真確的。請從您的瀏覽器直接輸入。這能避免您被引導至偽造網站。
  注意：滙豐金融不會在電郵或短訊中提供任何前往服務登入頁面的超連結。
- 滙豐金融沒有與任何第三方戶口整合應用程式有任何聯繫，基於安全考慮，客戶不應向任何第三方透露其網上交易服務個人認證資料，特別是一次性保安編碼。
- 僅使用信任的流動設備登入滙豐金融流動交易應用程式（「應用程式」），以確保您的戶口安全。
- 當登入服務後，請查閱上一次登入的時間和日期。此項資訊在服務的首頁提供。
- 不要讓瀏覽器儲存您的服務登入資訊。
- 您應經常核實網址的真確性。按下螢幕上方地址欄附近的「安全鎖」標誌，以確保網址的安全憑證為 www.hsbc.com.hk/broking/。
- 只從香港App Store 或 Google Play 下載應用程式，並確保應用程式的開發者為The Hong Kong and Shanghai Banking Corporation Ltd。這能確保您下載的應用程式是真實來自滙豐金融。
- 當您完成使用服務後，應按「登出」以確保在安全的情況下離開網站。
  注意：關閉瀏覽器視窗並不能確保您已經安全地離開服務網站。

- 切勿將您的密碼告訴任何人。
- 切勿將您的流動保安編碼或一次性密碼轉發給他人。
- 定期更改您的密碼（建議每個月更改一次）及選擇一個難以被人猜中的密碼。
- 設定新密碼時應選擇與以前十二次不同的密碼。
- 於不同的網頁及渠道應使用不同的密碼。
- 請默記您的私人密碼，不要寫下您的密碼。
- 謹記不要使用可由一般黑客程式拆解的密碼，如「password」一字、數字序列（如「 12345 」）、易於識辨的鍵次組合（如「14780」、「qwerty」）或常見單字。
- 避免與他人分享使用裝置，亦切勿使用他人的裝置登入您的私人戶口。
- 滙豐金融的職員絕不會向通過電話向您查詢密碼。滙豐金融亦不會以電話錄音的型式通知您戶口異常活動。

- 我們將會郵寄一個由系統產生的用戶識別碼 （「登記號碼」）及密碼（「登記密碼」）到閣下的通訊地址。您需要使用以上資料以完成服務的首次登記。請按此了解更多有關登記號碼及登記密碼的詳情。
- 您在登入服務時，您的服務受到獨有的1）用戶名稱；2）密碼；及3）第二密碼或由保安編碼器產生的一次性六位密碼所保護。請按此了解更多有關保安編碼器的詳情。
- 當您選擇使用「雙重密碼」模式登入服務及進行交易相關的活動或查詢個人資料時，您需要輸入由保安編碼器所產生或透過系統以短訊發送到閣下手提電話的一次性六位密碼（「保安編碼」），以加強身份認證。如閣下已更改手提電話號碼，請務必盡快更新於本公司所登記的手提電話號碼。請按此了解更多有關保安編碼的詳情。
- 當您成功透過服務執行以下活動後將會收到電郵提示：1）登入；或 2）更改密碼；或 3）發出交易指示。如您未曾執行電郵提示中提及的活動，請即致電客戶服務熱線與我們聯絡。如您已更改電郵地址，請務必盡快更新於本公司所登記的電郵地址。
- 基於安全考量，如果您一段時間在某個頁面都沒有進行任何操作，系統會自動登出服務。當您完成使用服務後，應該登出並關閉頁面。
- 我們一直致力確保您在使用服務時的安全。為此，我們將不再支援部份較舊的瀏覽器版本。一般而言，最新版本的瀏覽器（例如 Microsoft Internet Explorer, Google Chrome, Apple Safari）都支援最新的資訊保安技術。如果您還未安裝及使用最新版本的瀏覽器，請立即透過瀏覽器的網站進行版本更新。您可於網上搜尋相關操作說明。
- 在使用應用程式時，為確保更安全及更流暢的使用體驗，請更新至最新版本的應用程式。

- 所有人都應慎防網絡誘騙。網絡誘騙是犯罪分子的一種手段，旨在騙取安全認證資料等個人資料，或誘使點擊或打開惡意文件／連結。
- 您應安裝防火牆和防毒軟件，以防禦病毒和間諜軟件。大部分電腦均已預裝個人防火牆（又稱軟件防火牆）；您可另外下載一款獨立防火牆（又稱硬件防火牆），以提升安全水平。市面上的防毒軟件和防間諜軟件種類繁多，切記選用信譽良好的品牌，並提防偽冒產品。
- 經常查閱由滙豐金融發出的短訊、電郵提示、結單及電郵通知。
- 對任何外觀、感覺或內容與匯豐金融常規的短信 / 電郵 / 電話 / 網站不同的陌生短信 / 電郵 / 電話 / 網站保持警惕。留意電郵和網站的網域 (Domain)，如果您懷疑有任何網絡釣魚活動，請勿回復或點擊任何鏈接，或開啟任何附件。
- 確保您在滙豐金融所登記的手提電話號碼及電郵地址為有效及最新。
- 如果您對所顯示的資料有任何懷疑或收到任何可疑短訊 / 電郵 / 電話查詢您的登入或個人資料，請立即致電客戶服務熱線 (852) 3989 8181與我們的客戶服務主任聯絡。熱線服務時間為星期一至星期五（公眾假期除外）上午八時三十分至下午五時三十分。
- 有關更多網上保安資訊，請瀏覽滙豐金融網頁www.hsbc.com.hk/broking 內底部的「網上保安」 。

（本文件的資料將不時更新及只供參考。中英文版本如有歧義，概以英文版本為準。）